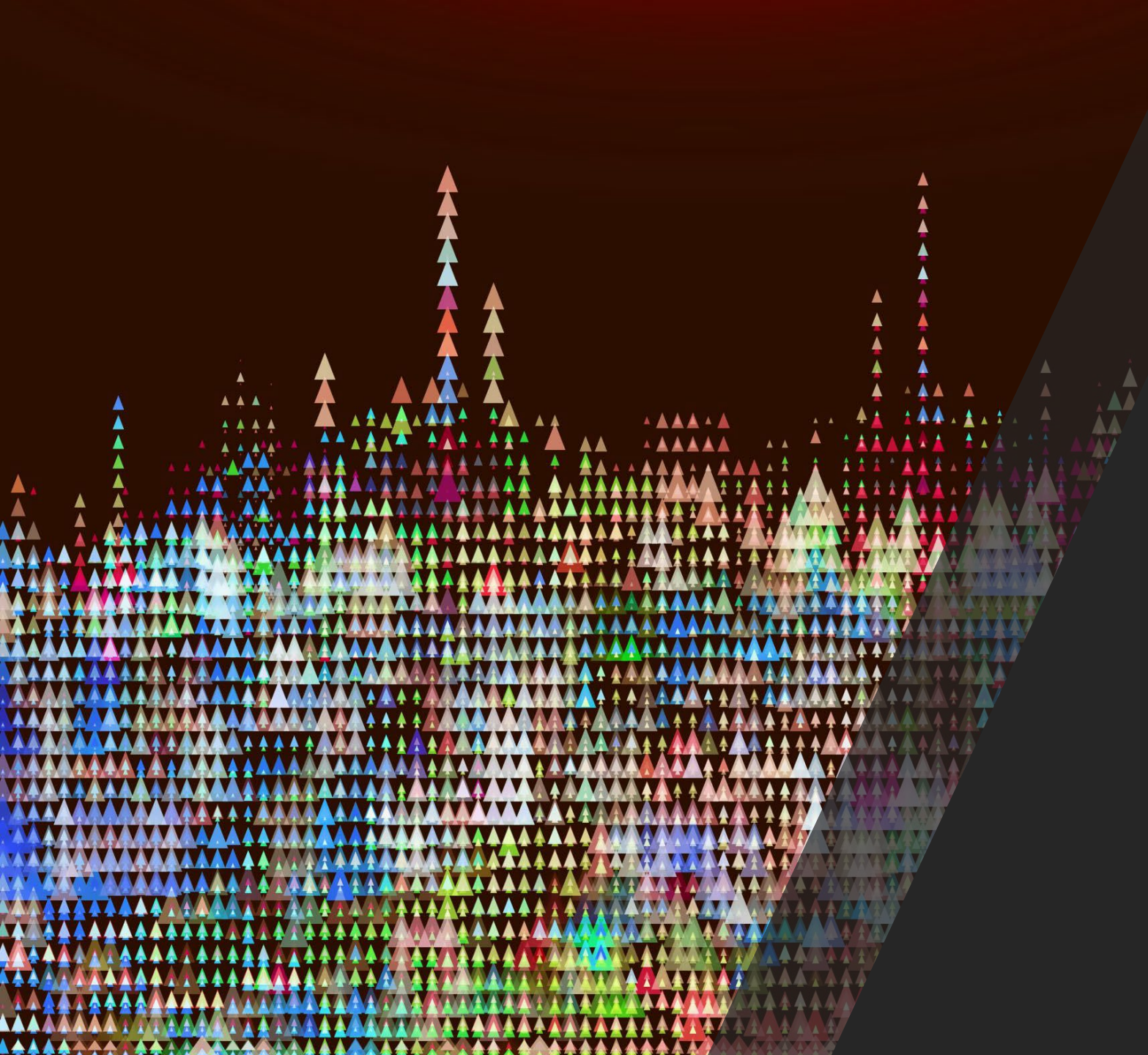
PROGRAM MATERIALS
Program #31136
June 3, 2021

Sequor Law Summer Series: De-Crypting Recovery of Cryptocurrencies 101; Trace it, Freeze it, Grab it

- Daniel M. Cole, Esq. - Sequor Law
- Amardeep Thandi - Control Risks Group Holdings Ltd.

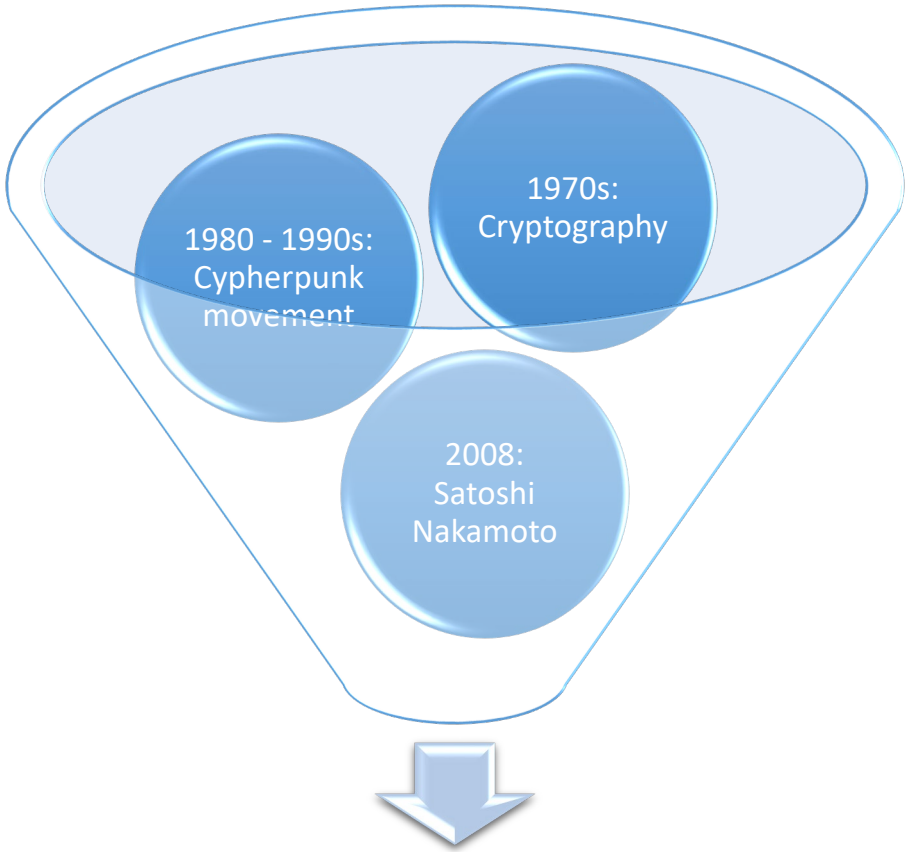
Celesq® AttorneysEd Center
www.celesq.com

5255 North Federal Highway, Suite 100, Boca Raton, FL 33487
Phone 561-241-1919

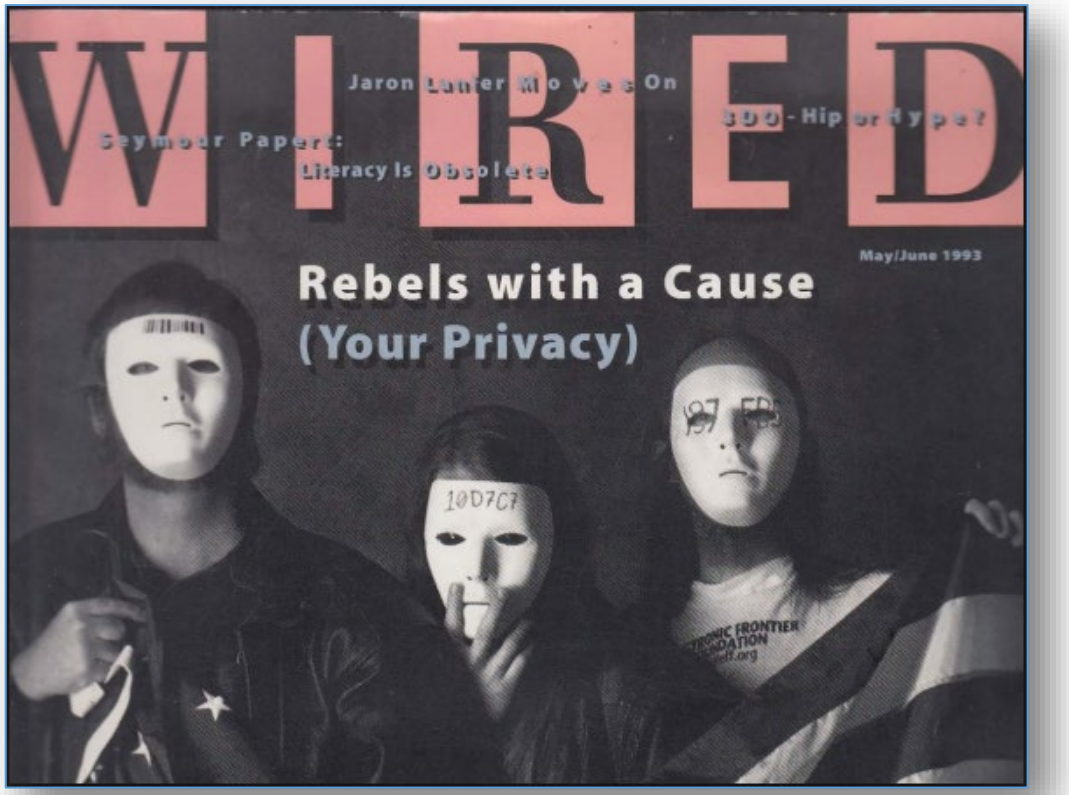


Crypto Currencies

Cypherpunk Movement – Pre-Bitcoin Era



2009: Bitcoin network

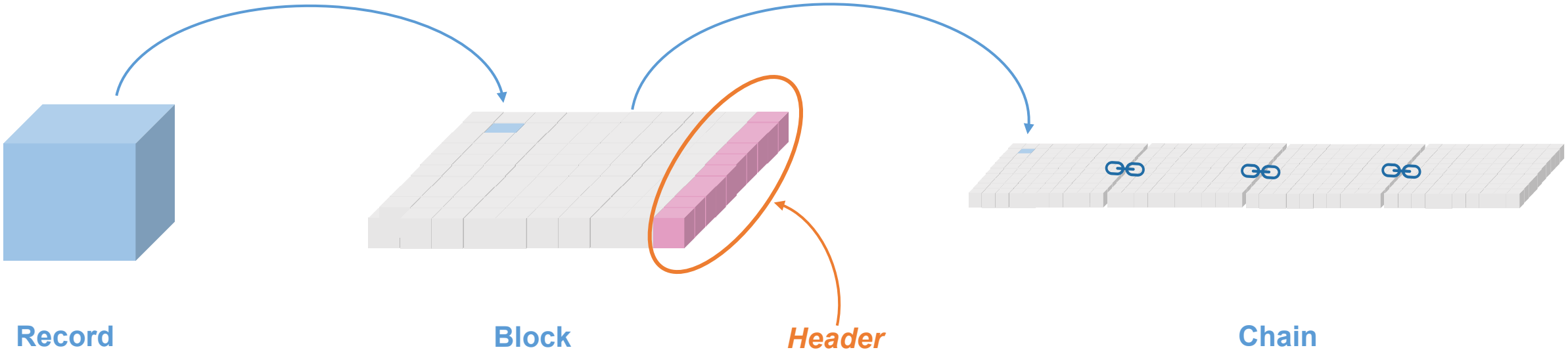


Cryptocurrency – Post Bitcoin Era

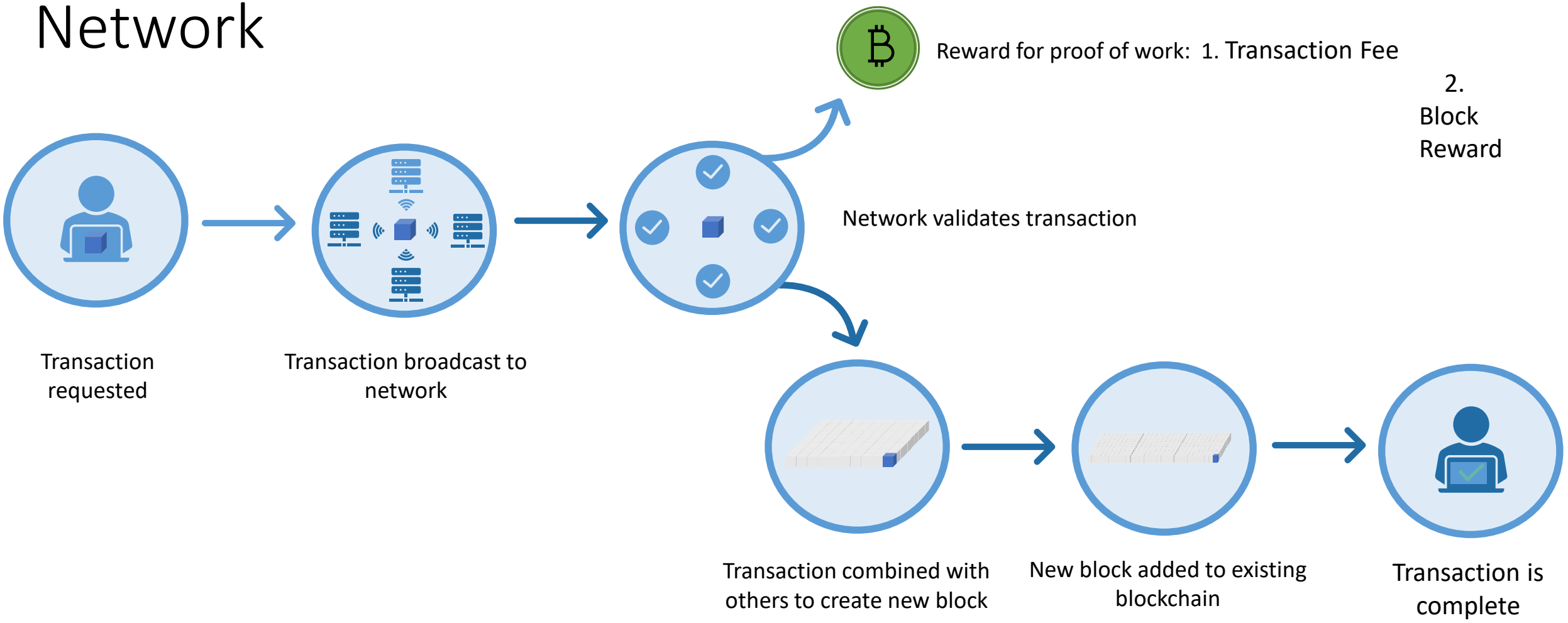
- 2011: competing cryptocurrencies emerge
- 2017 ICO Boom
- Bitcoins & Altcoins
- Stable Coins vs Currency vs stocks/shares
- 9000+ cryptocurrencies

Some Major CryptoCurrencies

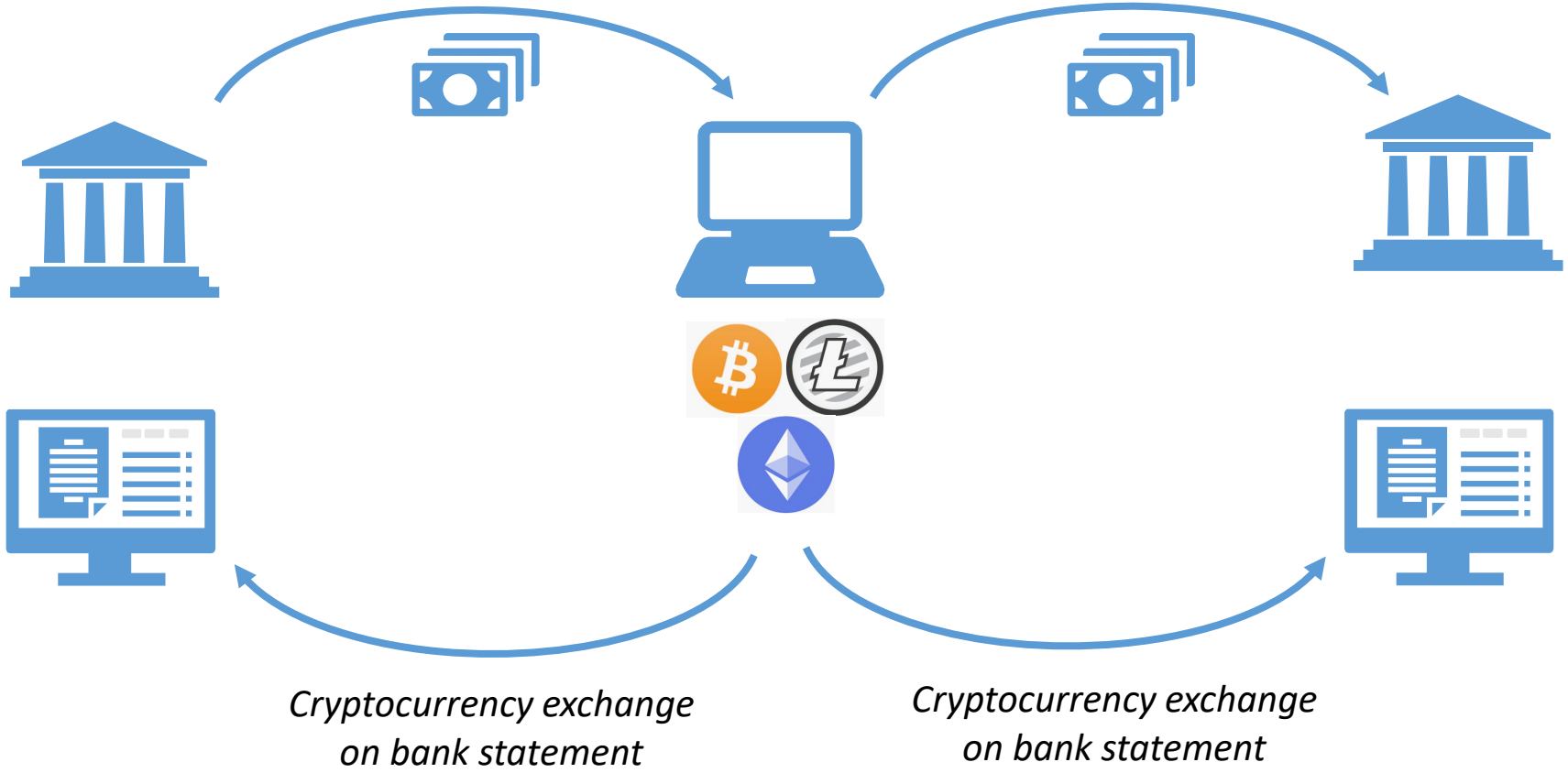
1. Bitcoin (BTC)
2. Ethereum (ETH)
3. Ripple (XRP)
4. EOS (EOS)
5. Bitcoin Cash (BCH)
6. Litecoin (LTC)
7. Chainlink (LINK)
8. Dogecoin (DOGE)


Record
Block
Header
Chain

DLT, Blockchain and The Bitcoin Network



Fiat vs Crypto - Entry and Exit Points



Some Major Exchanges

- 1. Binance: (HQ in Malta)
- 2. Coinbase: (HQ in San Francisco)
- 3. Coinjar: (HQ Melbourne)
- 4. Bittrex: (HQ in Seattle)
- 5. BitMEX: (HQ in Seychelles)
- 6. Blockgeeks: (HQ in Toronto)
- 7. Kraken: (HQ in San Francisco)
- 8. Quoine: (HQ in Tokyo)

Basics About Wallets

- Public Key - the address of the digital wallet
- Private Key - the password for the digital wallet
- Hot Wallets – online/actively connected to the internet
- Cold Wallets – offline/not actively connected to the internet

Stefan Thomas

Don’t Be This Guy

- A German-born programmer who lives in San Francisco. He forgot the password to his 7,002 Bitcoin fortune.
- Thomas lost the paper on which he wrote down his password, and only has 10 attempts before the IronKey encrypts its contents forever.

“Mixer” or “Blender” and “Chain Hopping”

Mixing/Blending:

- Intermediary service
- Takes in cryptocurrency from many sources
- Re-distributes the cryptocurrency back out in differing amounts to one or several accounts

Chain Hopping

- Exchanging one cryptocurrency for another
- Making tracing more difficult

Actors to Watch

- Hackers
- Organized Crime
- Payment Processors
- Exchanges

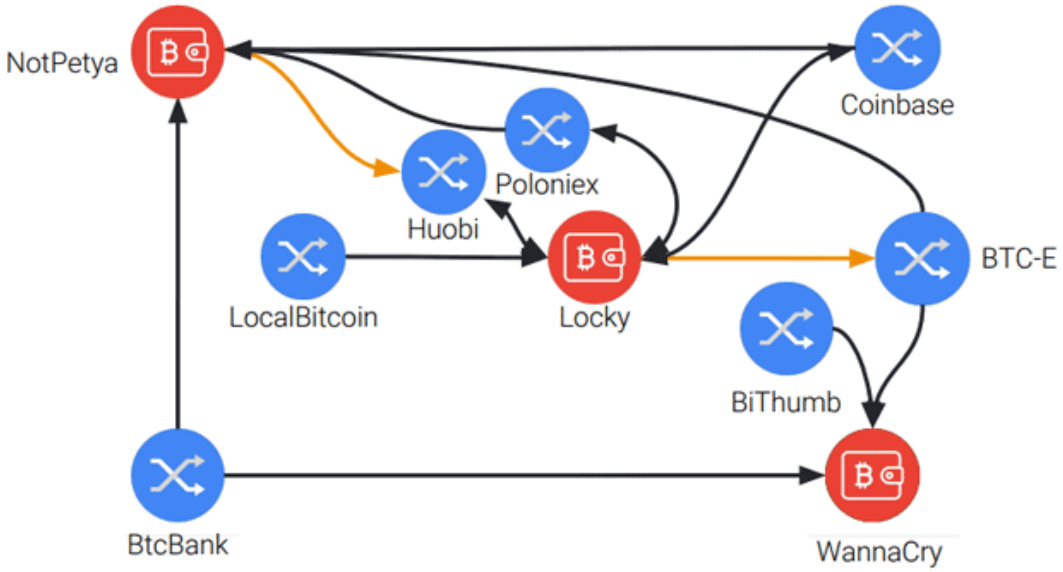
Cryptoforensic Tools

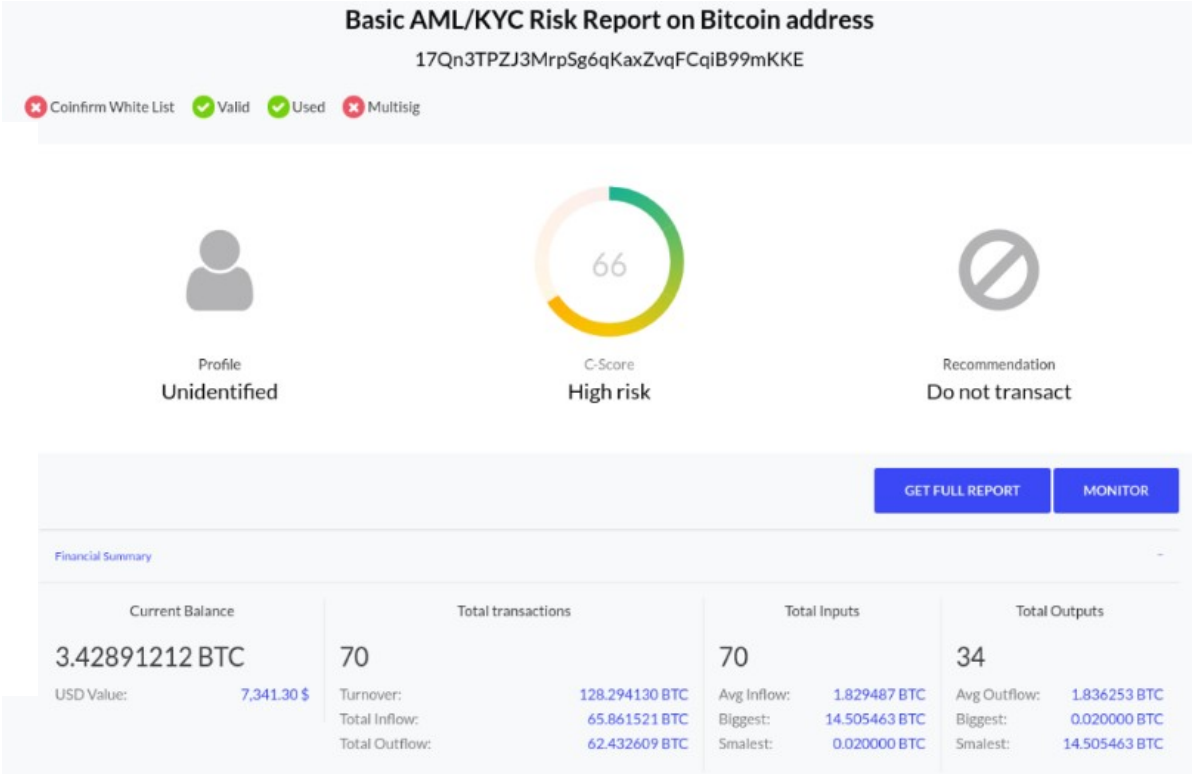
1. CHAINANALYSIS REACTOR
2. BLOCKCHAIN/ EXPLORER
3. CIPHERTRACE
4. DARKWEB SEARCHES
5. BITCOIN CORE (FORMERLY BITCOIN-QT)

The Investigation Process for Digital Forensic Science

1. Identification
2. Preservation
3. Collection
4. Analysis
5. Reporting

Developments – Forensic Technology





- *Ion Science and Duncan Johns v Persons Unknown; Binance Holdings Limited and Payment Ventures Inc.* [2020]

- High Court of Justice Business and Property Courts of England & Wales a Commercial Court
- No. CL-2020-000840

AA v Persons Unknown, iFINIEX trading as BITFINEX, and BFXWW INC trading as BITFINEX **[2019]**

- **EWHC 3665**
- **High Court**

Samara v Dan

[2019]

High Court Hong Kong Special Administrative Reg. HKCFI 2718

- *PML v Persons Unknown*

[2019]

- **High Court Of Justice Queen's Bench Division Media & Communications List**

Copytrack Pte Ltd. v Wall

[2018]

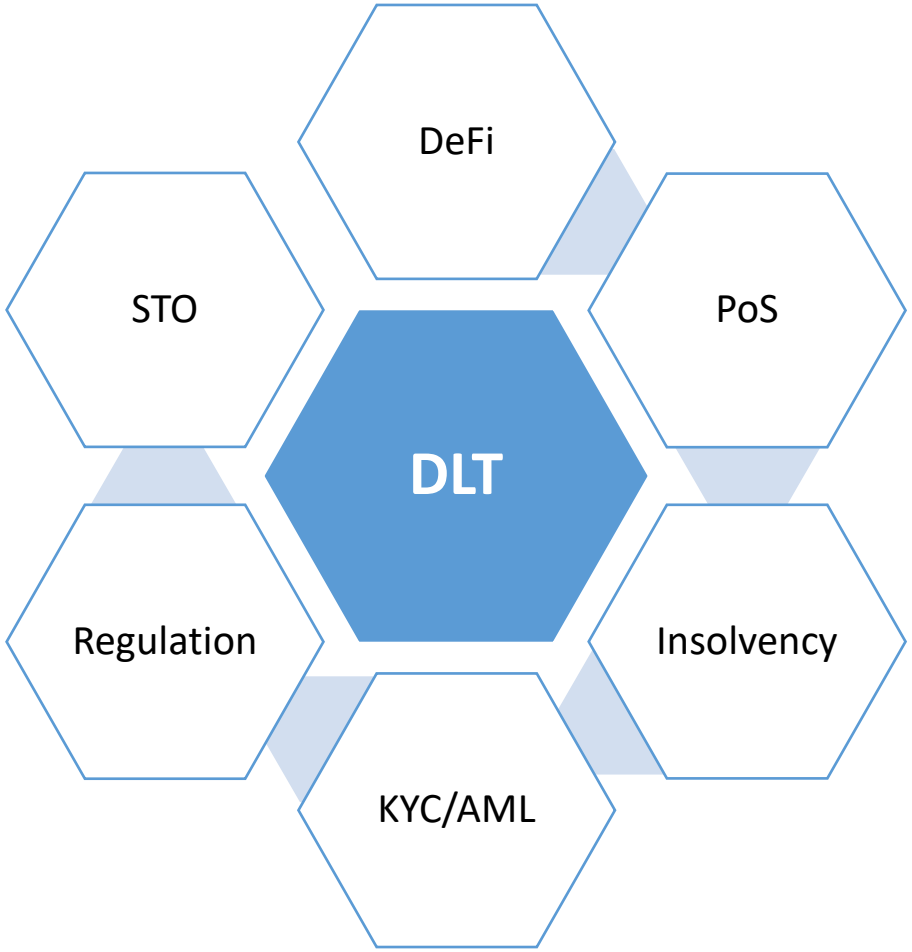
- **Supreme Court of British Columbia**
- **2018 BCSC 1709**

Dooga Ltd (Cubits) Redacted Order Granting Turnover (2020)

- United States Bankruptcy Court N.D. CA
- Case No. 20-30157-HLB

2021 Predictions in Crypto & DLT

- Bitcoin adoption will aid in £50 – 60k highs
- Defi, Yield Farming and Staking
- Increase in Crypto Payment partnerships
- ETH 2.0 & Scalability
- NFTs, Smart Contracts & tokenized assets



Copytrack Pte Ltd. v Wall, 2018 BCSC 1709 (CanLII)

Date: 2018-09-12
File number: S183051
Citation: Copytrack Pte Ltd. v Wall, 2018 BCSC 1709 (CanLII), <https://canlii.ca/t/hvddp>, retrieved on 2021-05-04

IN THE SUPREME COURT OF BRITISH COLUMBIA

Citation: *Copytrack Pte Ltd. v. Wall,*
2018 BCSC 1709

Date: 20180912
Docket: S183051
Registry: Vancouver

Between:

Copytrack Pte Ltd.

Plaintiff

And

Brian Wall

Defendant

Before: The Honourable Mr. Justice Skolrood

Oral Reasons for Judgment

In Chambers

Counsel for the Plaintiff:	B.J. Cabott
Counsel for the Defendant:	T.W. Clifford
Place and Date of Hearing:	Vancouver, B.C. May 22, 2018
Written Submissions of the Plaintiff:	June 12 and July 4, 2018
Written Submission of the Defendant:	July 4, 2018
Place and Date of Ruling:	Vancouver, B.C. September 12, 2018

Introduction

[1] **THE COURT:** The plaintiff, Copytrack PTE Ltd. ("Copytrack") is a Singapore company engaged in the business of digital content management and automated copyright enforcement. As part of its business, it created cryptocurrency known as “CPY Tokens”.

[2] From on or about September 10, 2017 to February 10, 2018, Copytrack offered CPY Tokens for sale to investors as part of an initial coin offering campaign (the “ICO”).

[3] The defendant Brian Wall (“Wall”) participated in the ICO and subscribed for 530 CPY Tokens. On or about February 15, 2018, Copytrack mistakenly transferred to Wall approximately 530 Ether Tokens (the “Ether Tokens”), which are a different form of cryptocurrency. The transfer was made to Wall's cryptocurrency wallet, referred to as the "Wall Wallet".

[4] The value of the CPY Tokens intended to be transferred was about $780 CDN. The value of the Ether Tokens that were transferred was about $495,000 CDN.

[5] Immediately after the erroneous transfer of the Ether Tokens to Wall, Copytrack advised Wall of the mistake and requested that he immediately return the Ether Tokens. To date, he has failed to do so. As I will discuss in further detail below, his position was that he no longer has possession or control of the Ether Tokens.

[6] This application is thus brought by Copytrack seeking a number of orders relating to what it says is Wall's wrongful retention or conversion of the Ether Tokens. Copytrack seeks summary judgment pursuant to Rule 9-6 of the *Supreme Court Civil Rules*. While Copytrack’s notice of civil claim alleges a number of different causes of action, its summary judgment application was limited to its claim for conversion and wrongful detention in respect of the Ether Tokens. To complicate matters, on May 25, 2018 I was advised by the parties that Wall had died on May 23, 2018, the day after Copytrack’s application was heard. I therefore asked counsel to provide me with written submissions on the impact, if any, of Wall's death. I also asked for additional submissions on the question of whether cryptocurrency is a “good” for the purposes of the doctrines of conversion and detinue. This latter point was only addressed in passing by the parties at the hearing.

Additional Facts

[7] While I have set out the basic facts underlying the proceeding, it is useful to highlight a few additional facts to complete the narrative.

[8] As noted, the mistaken transfer of the Ether Tokens occurred on February 15, 2018. On the same date, when the error was discovered, Copytrack requested the return of the Ether Tokens from Wall.

[9] Wall did not return the Ether Tokens, but rather transferred them into a cryptocurrency trading account with a cryptocurrency exchange.

[10] After some further email exchanges on February 16, 2018, Wall agreed to return the Ether Tokens. He asked Copytrack to provide him with the address to send the tokens to and Copytrack provided him with its cryptocurrency wallet address. Wall did not immediately return the Ether Tokens, however between February 16-23, 2018, the Ether Tokens were returned to the Wall Wallet.

[11] On February 25, 2018, the Ether Tokens were transferred out of the Wall Wallet into five different wallets. Wall asserts that these transfers were made by an unknown third party who unlawfully accessed his wallet without his knowledge or consent. This gives rise to his principal defence to Copytrack’s claim, namely that he no longer has control of the Ether Tokens and is therefore unable to return them.

Legal Framework

[12] Copytrack’s application is brought pursuant to Rule 9-6, subrule (5) of which provides:

> (5) On hearing an application under subrule (2) or (4), the court,
>
> (a) if satisfied that there is no genuine issue for trial with respect to a claim or defence, must pronounce judgment or dismiss the claim accordingly,
>
> (b) if satisfied that the only genuine issue is the amount to which the claiming party is entitled, may order a trial of that issue or pronounce judgment with a reference on an accounting to determine the amount,
>
> (c) if satisfied that the only genuine issue is a question of law, may determine the question and pronounce judgment accordingly, and
>
> (d) may make any other order it considers will further the object of these Supreme Court Civil Rules.

[13] In *Watson Island Development Corp. v. Prince Rupert (City)*, 2015 BCSC 1474 [*Watson*], Mr. Justice Dley provided a helpful summary of the principles governing an application under this Rule. At paras. 21 to 26 he stated:

> [21] The City applies under Rule 9-6 of the *Supreme Court Civil Rules*, B.C. Reg. 168/2009. Rule 9-6(5)(a) permits a court to dismiss a claim if it is satisfied that there is no genuine issue for trial.

Summary judgment may be granted on all or part of a claim. The onus is on the applicant to prove beyond a reasonable doubt that there is no triable issue: *Metro-Can Construction (HS) Ltd. v. Noel Developments Ltd.* (1996), , 1996 CanLII 3329 (BC CA), 26 B.C.L.R. (3d) 26 at para. 4; *Wong v. Wilson*, 2013 BCSC 1465 at para. 40. Another way of stating the test is whether the plaintiff is "bound to lose": *Pitt v. Holt*, 2007 BCSC 1555 at para. 10.

[22] The application under Rule 9-6 is based on the premise that the claim is factually without merit. It raises an issue of fact only or, at best, a question of mixed fact and law, unless the court determines under subrule (5)(c) that "the only genuine issue is an issue of law", in which case the court "may determine the question and pronounce judgment accordingly": *International Taoist Church of Canada v. Ching Chung Taoist Association of Hong Kong Limited*, 2011 BCCA 149 at para. 9.

[23] On an application under Rule 9-6 the court is not to weigh the evidence. If the evidence needs to be weighed and assessed, then the test of "plain and obvious" or "beyond a doubt" has not been satisfied and the application is to be dismissed: *Skybridge Investments Ltd. v. Metro Motors Ltd*, 2006 BCCA 500 at paras. 8-12; *International Taoist Church of Canada* at para. 14.

[24] An application to dismiss a claim that is bound to be unsuccessful weeds out unmeritorious claims and saves the heavy price of time and cost borne by the parties and the justice system: *4 Corners Properties Ltd. v. Boffo Developments (Smithe) Ltd.*, 2013 BCSC 1926 at para. 20.

[25] Caution must be exercised in granting summary judgment on only a portion of a claim so as to guard against litigating in slices: *Westsea Construction Ltd v. 0759553 BC Ltd.*, 2012 BCSC 564 (CanLII) at para. 49. Judgment on only a portion of the claim risks multiple appeals being heard within the same action, findings being made in the absence of a full factual context, and inconsistent findings being made after further evidence has been adduced: *Century Services Inc. v. LeRoy*, 2014 BCSC 702 at para. 89, var'd on other grounds 2015 BCCA 120.

[26] On the other hand, the resolution of an important part of the claim against a party may significantly impact the balance of the claim and provide for a timelier and cost effective approach: *Hryniak v. Mauldin*, 2014 SCC 7 at para. 60.

[Emphasis added.]

[14] In order to grant summary judgment, the Court must be satisfied that there is no genuine issue to be tried. The burden of establishing that there is no genuine issue to be tried rests with the party bringing the application.

Impact of Wall's Death

[15] Both parties submit that Wall's death does not affect Copytrack's claim. They cite s. 150 of the *Wills, Estates and Succession Act*, S.B.C. 2009, c. 13, the relevant provisions of which provide:

> 150 (1) Subject to this section a cause of action or a proceeding is not unknown by reason only of the death of
>
> (a) a person who had the cause of action, or
>
> (b) a person who is or may be named as a party to the proceeding.
>
> …
>
> (5) A person may commence or continue a proceeding against a deceased person that could have been commenced or continued against the deceased person if living, whether or not a personal representative has been appointed for the deceased person.
>
> …
>
> (8) All proceedings under this section bind the estate of the deceased person, despite any previous or subsequent appointment of a personal representative.

[16] In addition Rule 6-2(1) states:

> **Party Ceasing to Exist**
>
> (1) If a party dies or becomes bankrupt, or a corporate party is wound up or otherwise ceases to exist, but the claim survives, the proceeding may continue in spite of the death or bankruptcy of the corporate party having been wound up or ceasing to exist.

[17] I accept the parties' submissions that given these provisions, Copytrack's claim may proceed notwithstanding Wall's death.

[18] While Wall's death does not legally impact Copytrack's claim, it does have certain practical implications that I will return to.

Suitability for Summary Judgment

[19] An application for summary judgment requires that the Court first determine whether the matter is suitable for summary determination pursuant to the principles set out by Justice Dley in *Watson*.

[20] At the hearing of Copytrack's application, Wall submitted that the matter was not suitable for summary judgment as there are facts in dispute, specifically the facts relating to his failure or refusal to return the Ether Tokens and his allegation that his wallet was unlawfully accessed and that he therefore no longer had control of the Ether Tokens. He submitted further that the proper characterization of cryptocurrency and whether the doctrines of conversion and detinue are available with respect to cryptocurrency are questions of law that cannot be answered on a summary judgment application.

[21] Copytrack submits that there is no *bona fide* issue for trial. It submits that it is clear on the uncontradicted evidence that the Ether Tokens were sent to Wall in error and that he has no proprietary interest in them. Copytrack submits further that Wall has simply made a bald and unsubstantiated assertion that the Ether Tokens were stolen by an unknown third party and that, in any event, the loss of control over the tokens is not a defence given that he failed or refused to return the tokens when demand was made and while they were still in his control.

[22] I do not accept Wall's submission that there are factual disputes that make summary judgment unavailable. The essential facts underlying Copytrack's claim are undisputed. Specifically, I do not accept Wall's submission that the application involves "oath against oath", particularly given that Wall's evidence about what happened to the Ether Tokens amounts to little more than a bald assertion. Moreover, Wall does not in his amended response to civil claim assert that he has any proprietary interest in the Ether Tokens that, if established, would defeat Copytrack's claim.

[23] Further, given Wall's death, it is not clear what sending this matter to trial would accomplish since it would not result in further or better evidence on behalf of the defendant.

[24] The real issue on this application is whether the doctrines of conversion and wrongful detention apply and whether that issue can be determined on a summary judgment application.

[25] At the initial hearing, Copytrack's submission was based on the premise that Ether Tokens are "goods". For example, at para. 89 of its written submission, it set out the elements of an action in detinue for the recover of "goods" wrongfully converted or detained. It then structured its submissions to address the elements of the test, and submitted that it "has a better right to the goods than the defendant", that it "has requested return of the goods" and that the defendant has refused that request. Nowhere in its submission did Copytrack address the question of whether cryptocurrency, including the Ether Tokens, are in fact goods or the question of if or how cryptocurrency could be subject to claims for conversion and wrongful detention. The submission simply assumed that to be the case.

[26] That issue was however raised by counsel for Wall in his oral submission, virtually in passing, who noted that there are no decided cases dealing with this point.

[27] Given the manner in which this issue was addressed at the hearing, I requested additional submissions from the parties. I pause here to note that it was open to the Court to simply dismiss Copytrack's summary judgment application on the basis of its failure to address what I consider to be a critical issue. However, given that the application had been fully argued in other respects, and the fact of Wall's death which made a trial untenable, the preferred approach was to permit additional submissions on this point.

[28] In its further submission, Copytrack, having initially staked its position essentially on the assumption that Ether Tokens are goods, now takes the position that a broad range of things can be subject to claims in conversion and detinue and that a determination that cryptocurrency is a good is in fact unnecessary. Copytrack cites various cases in which such claims have been advanced in relation to funds, shares, customer lists, accounts receivable, crops and mineral interests.

[29] Copytrack points in particular to the decision of Mr. Justice Walker in *Li v. Li*, 2017 BCSC 1312 [*Li*], where he found that funds may be subject to a claim of conversion, which he described at para. 213 as a "positive

wrongful act of dealing with goods, including funds, in a manner and with an intention inconsistent with the owner's rights".

[30] Copytrack submits that the evidence establishes that the Ether Tokens have the following characteristics:

a) They are capable of being possessed, stored, transferred, lost and stolen;

b) They were, at the time the conversion and wrongful detention began, held in the Wall Wallet;

c) They are specifically identifiable and have been traced to five wallets in which they are currently being held; and

d) They can be used as a medium of exchange, a store of value, and a unit of account, like funds or currency.

[31] Copytrack submits that given these characteristics, the Ether Tokens can in fact be subject to a claim in detinue based on wrongful conversion or detention.

[32] In the additional submission filed on behalf of Wall, it is submitted that the characterization of cryptocurrency, and whether cryptocurrency is subject to claims of conversion and/or detinue, is a pure question of law that cannot be decided on a summary judgment application.

[33] Various dictionary definitions are cited that suggest that cryptocurrency is not, in fact, a "good" but rather a digital form of currency. However, the defendant submits that cryptocurrency is distinguishable from the type of specific funds dealt with in cases like *Li*.

[34] In my view, the proper characterization of cryptocurrency, including the Ether Tokens, is a central issue in this case, and one that informs the analysis of whether Copytrack's claims in conversion and detinue can succeed. However, the evidentiary record is inadequate to permit a determination of that issue on this application, and, in any event, it is a complex and as of yet undecided question that is not suitable for determination by way of a summary judgment application.

[35] However, as I have indicated, there would be no practical utility in sending this matter to trial given Wall's death. Further, regardless of the characterization of the Ether Tokens, it is undisputed that they were the property of Copytrack, they were sent to Wall in error, they were not returned when demand was made and Wall has no proprietary claim to them. While the evidence of what has happened to the Ether Tokens since is somewhat murky, this does not detract from the point that they should rightfully be returned to Copytrack.

[36] In the circumstances, it would be both unreasonable and unjust to deny Copytrack a remedy.

[37] In my view, the appropriate remedy is therefore that set out in para. 1(c) of Cophytrack's notice of application as follows:

> An order that Copytrack be entitled to trace and recover the 529.8273791 Ether Tokens received by Wall from Copytrack on 15 February 2018 in whatsoever hands those Ether Tokens may currently be held.

[38] That is the order that I am prepared to make. The balance of the relief sought in the notice of application, for example, disgorgement and/or damages, is not appropriate for summary judgment and those aspects of the application are dismissed. Those are my reasons.

(Submissions on Costs)

[39] THE COURT: I am going to order costs payable, which may ultimately be from the estate, for this application only, to the plaintiff.

"Skolrood J."

Neutral Citation Number: [2019] EWHC 3556 (Comm)

Case No: CL-2019-000746

IN THE HIGH COURT OF JUSTICE
BUSINESS & PROPERTY COURTS OF ENGLAND AND WALES
COMMERCIAL COURT (QBD)
IN PRIVATE
(reporting restrictions lifted,
and released for publication, 17 January 2020)

The Rolls Building
7 Rolls Buildings
Fetter Lane
London EC4A 1NL

Date: Friday, 13th December 2019

Before:

THE HONOURABLE MR. JUSTICE BRYAN

- -

Between:

AA	**Claimant**
- and -	
(1) PERSONS UNKNOWN WHO DEMANDED BITCOIN ON 10TH AND 11TH OCTOBER 2019 **(2) PERSONS UNKNOWN WHO OWN/CONTROL SPECIFIED BITCOIN** **(3) iFINEX trading as BITFINEX** **(4) BFXWW INC trading as BITFINEX**	**Defendant**

- -
- -

MR. DARRAGH CONNELL (instructed by **Brandsmiths SL Ltd**) for the **Claimant**

- -

APPROVED JUDGMENT

MR. JUSTICE BRYAN:

INTRODUCTION

1. There is before me today an application made by an applicant, an English insurer who requests to be anonymised, against four defendants. Those four defendants are: the first defendant, persons unknown who demanded Bitcoin on 10th and 11th October 2019; the second defendant, persons unknown who hold/controls 96 Bitcoins held in a specified Bitfinex Bitcoin address; the third defendant, iFINEX Inc trading as Bitfinex; and the fourth defendant, BFXWW INC also trading as Bitfinex.

BACKGROUND

2. The application relates to the hacking of a Canadian insurance company that I will refer to simply as the Insured Customer. What happened in relation to that company is that a hacker managed to infiltrate and bypass the firewall of that insured customer, who happens to be an insurance company, and installed malware called BitPaymer. The effect of that malware was that all of the insured customer's computer systems were encrypted, the malware having first bypassed the system's firewalls and anti-virus software. The Insured Customer then received notes which were left on the encrypted system by the first defendant. In particular, there was a communication from the first defendant as follows:

> "Hello [insured customer] your network was hacked and encrypted. No free decryption software is available on the web. Email us at […] to get the ransom amount. Keep our contact

> safe. Disclosure can lead to impossibility of decryption. Please use your company name as the email subject."

3. The Insured Customer is insured with the applicant, (an English insurer), whom I shall refer to as "the Insurer"/"the Applicant". The Insurer is applying to be anonymised for reasons that I will come on to. The Insurer instructed, as is common in such cases, what is known as an Incident Response Company (IRC) that specialises in the provision of negotiation services in relation to crypto currency ransom payments. The Insured Customer is insured with the Insurer against cyber crime attacks.

4. That entity, IRC, then was instructed by the Insurer to correspond with the first defendant on behalf of it and the Insured Customer so as to negotiate the provision of the relevant decryption software (the tool) which would allow the Insured Customer to re-access its data and systems. Following initial emails from IRC asking the first defendant: "*To relay your terms of decryption*" the first defendant stated *"Hello, to get your data back you have to pay for the decryption tool, the price is $1,200,000 (one million two hundred thousand). You have to make the payment in Bitcoins."*

5. After several exchanges the first defendant agreed the value of the payment to recover the tool as follows:

> "as an exception we can agree on US $950K for the tool. You can send us a few encrypted files for the test decryption ((do not forget to include the corresponding _readme files as well)."

6. Given the importance to the Insured Customer to obtain access to its systems, the Insurer agreed to pay the ransom in return for the tool.

7. In further correspondence which is exhibited before me, and following the testing of several encrypted files, the first defendant stated as follows:

> "The Bitcoin address for the payment […] When sending the payment check the USD/BTC exchange rate on bitrex.com we have to receive no less than USD 950K in Bitcoins. It takes around 40-60 minutes to get enough confirmations form [sic] the blockchain in order to validate the payment. Upon receipt we send you the tool."

8. The payment of the ransom in Bitcoin was via an agent of the Insurer, who was referred to as JJ, and who assists with the purchase and transfer of crypto currencies, including Bitcoins. Acting on the Insurer's instructions and with its authority JJ purchased and transferred 109.25 Bitcoins to the address that was provided.

9. The ransom was subsequently paid at 12.24 on 10th October 2019 and by way of email IRC requested confirmation from the first respondent:

> "Please reply. You have received $950,000 and I am hoping we can get what we need ASAP. Thank you."

10. The tool was indeed received on 11th October 2019 at 04.07 pacific daylight time by way of the following message:

"Hello,

Here is the tool

Download

[address]

Delete:

[address]

Password:

[address]

Execute the tool on every impacted host"

11. The tool was a click through application that had to be executed on each of the Insured Customer's encrypted systems. The time it took to decrypt the data varied from system to system due to the quantity of the files on each system and the system's own resources, like processor and memory. The information before me is that it took decryption of 20 servers of the Insured Customer five days and 10 business days for 1,000 desktop computers.

12. Following the payment of the ransom and the provision of the decryption tool, further investigations were undertaken on behalf of the Insurer by an employee who is also the deponent of an affidavit, dated 3rd December, in support of the various applications that are made before me.

13. Those investigations involved contacting a specialist company who is a provider of software to track payment of crypto currency. That company is Chainalysis Inc, which is a blockchain investigations firm operating in New York, Washington DC, Copenhagen, and London. They are known in the public domain not least because their work was referred to in a recent High Court case of *Liam David Robertson v Persons Unknown,* CL-2019-000444, unreported, 15th July 2019, a decision of Moulder J, where she relied upon an analysis provided by that entity to track 80 Bitcoin to a wallet/account/address held by a crypto currency exchange called "Coinbase".

14. In the present case, it was possible to track the Bitcoins that had been transferred as a ransom. Whilst some of the Bitcoins was transferred into "fiat currency" as it is known, a substantial proportion of the Bitcoin, namely, 96

Bitcoins, were transferred to a specified address. In the present instance, the address where the 96 Bitcoins were sent is linked to the exchange known as Bitfinex operated by the third and fourth defendants.

15. The Insurer is unable to identify the second defendant from the Bitcoin address referred to but that is information which is either held or likely to be held by the third and fourth defendants, to comply with their Know Your Customer ("KYC"), an anti-money laundering requirement.

APPLICATION FOR HEARING TO BE IN PRIVATE

16. Set against that background the first application that was made before me was for this hearing to be in private. The important principle of open justice is one which is well established. The origins and the rationale, for the principle, was stated by Lady Hale in *Cape Intermediate Holdings Ltd v Dring* [2019] UKSC 38, at [42] and [43], referring to *Scott v Scott* [1931] AC 417.

17. The relevant provision of the CPR is CPR 39.2, which provides:

> "39.2(1) The general rule is that a hearing is to be in public. A hearing may not be held in private irrespective of the parties' consent unless and to the extent that the court decides it must be held in private applying, the provisions in paragraph (3).
>
> "39.2(2) In deciding whether to hold a hearing in private the court must consider any duty to protect or have regard to a right to freedom of expression which may be affected."

18. CPR.39.2 was recently amended by the addition of a new subparagraph (2A) which provides:

> "The court shall take reasonable steps to ensure that all hearings are of an open and public character save when a hearing is held in private."

19. Subparagraph 39.2(3) provides:

> A hearing, or any part of it, must be held in private if, and only to the extent that, the court is satisfied of one or more of the matters set out in sub-paragraphs (a) to (g) and that it is necessary to sit in private to secure the proper administration of justice—
>
> (a) publicity would defeat the object of the hearing;
>
> (b) it involves matters relating to national security;
>
> (c) it involves confidential information (including information relating to personal financial matters) and publicity would damage that confidentiality;
>
> (d) a private hearing is necessary to protect the interests of any child or protected party;
>
> (e) it is a hearing of an application made without notice and it would be unjust to any respondent for there to be a public hearing;
>
> (f) it involves uncontentious matters arising in the administration of trusts or in the administration of a deceased person's estate; or
>
> (g) the court for any other reason considers this to be necessary to secure the proper administration of justice.

20. The test is one of necessity and not of discretion: see *AMM v HXW* [2010] EWHC 2457 (QB), per Tugendhat J. This is reflected in the wording of rule 39.2(3), such that a hearing or part of a hearing must be held in private if the court is satisfied that one or more of the factors specified in the subparagraphs (a) to (g) are satisfied and it is necessary to sit in private to secure the proper administration of justice. The court also needs to consider proportionality, namely whether the proper administration of justice can be achieved by a lesser measure or combination of measures such as imposing reporting restrictions, anonymising the parties, or restricting access to court records. This is because a private hearing will restrict the exercise of the Article 10 Convention right of freedom of expression, through prohibiting the disclosure of information.

21. It is well established, as is acknowledged in this case by the Insurer, that the general principle that hearings be held in public is not to be lightly departed from in respect of civil proceedings. It is submitted, however, that there are compelling grounds, supported by credible and cogent evidence, as to why in this particular, and unusual, case the hearing should be held in private, relying upon the grounds specified in 39.2(3)(a) (c) (e) and/or (g).

22. First of all, in terms of publicity, it is said that publicity would defeat the object of the hearing. The overarching purpose of the application is to assist the applicant in its efforts to recover crypto currency in the form of the 109.25 Bitcoins that were unlawfully extorted pursuant to what is characterised as an extortion/blackmail, perpetrated on the 10th and 11th October against the Insured Customer and resulting in financial loss to the Insurer.

23. If the hearing were to be held in public there is a strong likelihood that the object of the application would be defeated. First of all, there would be the risk, if not the likelihood, of the tipping off of persons unknown to enable them to dissipate the Bitcoins held at the second defendant's account with Bitfinex, the real possibility of reprisal or revenge cyber attacks on either the Insurer or indeed the Insured Customer by persons unknown, the possibility of copycat attacks on the Insurer, and/or the Insured Customer and the revealing of confidential information considering the Insurer's processes and the Insured Customer's systems which will be necessary on this application, in circumstances where the vulnerability of those very systems form the basis for the blackmail itself. Ultimately, the applicant contends it is necessary for the court to sit in private to secure the proper administration of justice.

24. There are previous authorities touching upon such matters. For example, in cases concerning blackmail - and this is certainly analogous to that, a ransom is being demanded and money is being extorted in return for the decrypting of computer systems - it is more common for the court to permit hearings to be held in private. This is because the interests of freedom of expression are naturally tempered by the criminal conduct in question and the presence of blackmail will be an important factor and matter in determining privacy applications where injunctive relief is sought to thwart blackmailers as was noted by Warby J in *LJY v Persons Uknown* [2018] EMLR 19 at [29]:

> "Generally, the court has taken the view that blackmail represents the misuse of freedom of speech rights. Such conduct will considerably reduce the weight attached to free speech and correspondingly increase the weight of the arguments in favour of restraint. The court recognises the need to ensure that it does not encourage or help blackmailers or deter victims of blackmail from seeking justice before the court. All these points are well recognised ."

25. It has also been recognised that these considerations apply in the event of ransom funds having <u>already</u> been paid. That was emphasised in *NPV v QEL* [2018] EMLR 20 where the court permitted an interim application to be heard in private in the context of the ongoing blackmail of a businessman who demonstrated at least a prima facie case that he had already been blackmailed and an attempt was being made to continue that blackmail effort to obtain more money. It was held in that case that the court had to *"adapt its procedures"* to ensure that it neither encouraged nor assisted blackmailers nor deterred victims of blackmail from seeking justice from the courts. If the application had been heard in public the information which the claimant was trying to protect would have been destroyed by the court's own process.

Further, at least until the return date when the issue could be reconsidered, the defendants would also be anonymised. The claimant was making serious allegations against the defendants and they had not yet had an opportunity to respond.

26. It is said of particular relevance in present case is the case of *PML v Persons Unknown* [2018] EWHC 838 QB. In that matter, PML was the victim, as here, of a cyber attack by unknown hackers demanding £300,000 worth of Bitcoin and in default of payment certain information would be publicly disseminated. PML made an interim application for, amongst other things, an interim anonymity order and orders to restrain the threatened breach of confidence and for delivery up and/or destruction of the stolen data.

27. At the interim hearing which came before me, I sat in private and granted the injunction. In doing so I made a series of further orders, including anonymising the claimant and restricting access to the court files. I was satisfied that the requirements of section 12(3) of the Human Rights Act 1998 were met. I was also satisfied that the requirements under section 12(2) of the same Act were met, where the claimant appeared to be a victim of blackmail and there was a risk that, were the defendant to be given notice of the application, he would publish the relevant information and there were compelling reasons why the defendant had not been notified of the application. At the return hearing the court ordered the application continue to be heard in private as the judge on the return date, Nicklin J, was satisfied that it was strictly necessary to hear the application in private pursuant to CPR 39.3 (a) (c) and (g). Of particular relevance was that the purpose of the proceedings

would have been frustrated, or at least harmed, had the hearing been conducted in public. It was necessary for the court to hear evidence and submissions relating to the blackmail activities of the persons unknown along with the nature of the attack in question.

28. In the present case it is said that confidential material is involved, including details of the confidential cyber insurance policy held by the customer, the precise mechanism by which the cyber attack occurred, details of the confidential internal procedures of the Insurer and details of the way in which the Insurer had discovered the location of the Bitcoins, although I recognise that a number of those pieces of information are probably in the public domain in any event (at the level of detail which I have identified them), although further confidential information is also before me which I have had to consider.

29. A recent example of a commercial case in which the court permitted the hearing of the application for interim relief in private is *Taher v Cumberland* [2019] EWHC 2589 QB. In that case the court granted an order for the hearing of a committal application be heard in private for reasons which were set out at [76] of the judgment:

> "I heard the Privacy Application at the beginning of the hearing, giving reasons in public for granting it, which I summarise as follows:
>
> i) The Orders are principally concerned with preventing the defendants and, in particular, Mr Cumberland, directly or indirectly, from making or encouraging the making of disparaging statements about the claimants or in other ways acting to damage the business or reputation of the claimants. It will be necessary during the course of the hearing to consider various allegations and allegedly damaging statements made by Mr Cumberland, his motivations for making them and other relevant circumstances, the ventilation of which could have the damaging effect of which it is the purpose of this claim to prevent or avoid.

> ii) I was satisfied that the grounds set out in CPR 39.2(a) , (c) and (g) apply to this case and justify the hearing of the matter in private.
>
> iii) I considered whether it was necessary and proportionate to conduct the hearing in private or whether some lesser measure or combination of measures would suffice, such as imposing reporting restrictions, anonymising the parties or restricting access to court records. I was satisfied, however, that no lesser measure or combination of measures would provide the necessary protection, given the nature of the conduct alleged against Mr Cumberland (much of which, I note, he admitted during the course of the hearing) which would make it difficult, if not impossible, for the court effectively to police and enforce lesser measures.
>
> iv) I found it relevant to these considerations that the business of the claimants is one in which the reputation of the companies and of the leading individuals managing and operating them are of critical importance. Damage to reputation can lead to rapid and potentially massive losses for a business operating in the international financial services sector."

30. I am satisfied that this is an appropriate case for the hearing to be heard in private, as I indicated at the start of the hearing saying I would give reasons in due course. My reasons are given now. First of all, I am satisfied for the purpose of CPR 39(3) that publicity would defeat the object of the hearing. It would potentially tip off the persons unknown to enable them to dissipate the Bitcoins; secondly, there would be the risk of further cyber or revenge attacks on both the Insurer and the Insured Customer by persons unknown; there would be a risk of copycat attacks on the Insurer and/or the Insured Customer and I am satisfied that in all the circumstances it is necessary to sit in private so as to secure the proper administration of justice.

31. In terms of the application itself and the hearing before me, I am also satisfied that limb (c) is also applicable because during the course of this hearing I was provided with confidential information which I have not repeated during the course of this judgment and it was necessary for me to hear that confidential information properly to rule upon this application.

32. Equally, (e) applies, it is as hearing of an application made without notice and it would be unjust for any respondent to be referred to in a public hearing. That applies, in particular, to the third and fourth defendants who have not yet had an opportunity to address this court, and as will become apparent, at the very least they have, by the nature of the Exchange that they run, become mixed up in the wrongdoing, perpetrated by the first and second defendants.

33. I am satisfied that the sentiments expressed by Warby J in *LJY* apply here. It is important in the context of blackmail and extortion that those who have suffered such wrongs should not be put off approaching the court and should be offered assistance in such circumstances, and blackmail itself represents a misuse of free speech, which will mean that the interests of justice and the interests of freedom of expression are naturally tempered by the civil and potentially criminal conduct in question. I consider for the same reasons as I gave in the *PML* case that the requirements under section 12 of the Human Rights Act are also met in the present case.

34. For very much the same reasons I am also satisfied that this application was properly made without notice to the first and second defendants. Again, by the very nature of the relief sought, if the first and second defendants had been notified of this application, then steps could have been taken to thwart any order by moving the Bitcoins. These concerns are particularly important in the context of virtual currencies such as Bitcoin because they can be moved literally at the click of a mouse.

35. So far as the position of the third and fourth defendants are concerned, this application is actually made ex parte on notice, by that I mean that the third

and fourth defendants, who are effectively the Exchange, who are holding the Bitcoin, were notified of this application. I consider that it was appropriate to do so although they are mixed up, it is said, in the wrongdoing and indeed it is said on behalf of the claimant, as I shall come on to, that in fact there is a cause of action against them in the form of a restitutionary claim or a constructive trust. Essentially, they have become mixed up in this wrongdoing. At the present time there is no evidence that they are themselves perpetrators of the wrongdoing, rather, it is said, they have found themselves the holder of someone else's property, or at least that is how it is characterised for the purpose of this application by the claimant, with the result that there may be claims against them for restitution or as constructive trustees vis a vis, the Insurer.

36. I also consider it is appropriate to anonymise the Insurer in the terms that I have identified, again because of the risk of retaliatory cyber attacks upon the Insurer just as much as upon the Insured Customer.

37. It is likely that once the first and second defendants are served and/or the property is protected, I will lift the privacy in respect of this judgment so that it can be publically reported. It has been drafted in terms that will allow that to be done. The public reporting of judgments is an important aspect of the principle of open justice.

NORWICH PHARMACAL/BANKERS TRUST APPLICATION

38. Turning then to the nature of the claims and the relief that is sought, as the application came before me the following relief was sought. First of all, a Bankers Trust order and/or a Norwich Pharmacal order requiring the third and

fourth defendants to provide specified information in relation to a crypto currency account owned or controlled by the second defendant; and/or, a proprietary injunction in respect of the Bitcoin held at the account of the fourth defendant; and/or, a freezing injunction in respect of Bitcoin held at the specified account of the third or fourth defendant; and consequential orders to serve the same, including alternative service and service outside the jurisdiction.

39. As is rightly noted in the supporting skeleton argument, this application raises certain novel legal issues relating to crypto currencies. In this regard, the court has recently grappled with analogous issues in the cases of *Vorotyntseva v Money-4 Limited, trading as Nebeus.com* [2018] EWHC 2598 (Ch), a decision of Birss J, and *Liam David Robertson v Persons Unknown* (unreported 15th July 2019) a decision of Moulder J. In addition, my attention has been referred to the recent legal statement of the UK jurisdiction Task Force "Crypto Assets and Smart Contracts" dated 11th November 2019, about which more in due course.

40. During the course of oral argument before me, I explored in some considerable detail with Mr. Darragh Connell, counsel, who appears on behalf of the claimant Insurer, in relation to precisely what causes of actions were claimed, and what jurisdictional gateways there were for service out of the jurisdiction in relation to each of the claims.

41. Another point that arose and which I explored with Mr. Connell was in relation to the application for Bankers Trust or Norwich Pharmacal type relief against an entity (the two entities which are D3 and D4) who are out of the

jurisdiction. It appears they are in fact BVI companies, although a number of their officers, including the chief financial officer and the chief technical officer, have close association with this jurisdiction, indeed it appears that the chief financial officer may be resident in this jurisdiction and that the chief technical officer has at least some association with this jurisdiction.

42. When corresponding with the third and fourth defendants putting them on notice of this application, an address in China was also identified. It is fair to say that D3 and D4, at the moment at least, have cooperated with the claimant in the following sense, which is that in email correspondence they have indicated that they are not able to comply with any order to identify anyone associated with the account, absent a court order, but that it is their practice to comply with the court order for any national jurisdiction. They had initially said that they were prepared to accept service by email which is their normal method of service but I have now been shown an email on 4th December 2019 whereby they have said they are required to be served in the British Virgin Islands.

43. In light of that there is also an application for alternative service against them using the email addresses with which there has been communication. I should also say that those communications copy in counsel from a set of chambers in London. It is assumed, therefore, that they have London counsel, although enquiries were made this morning to ensure that counsel was not attending and the message that was passed back to me was that they did not have any instructions to attend on the application. It is fair to say, therefore, that on the

application, so far as the third and fourth defendants were aware of it, adopted an essentially neutral stance in relation to the applications.

44. As I say, I have explored with Mr. Connell both the causes of action that his client has and also the jurisdictional gateways which he relies upon for his various claims for relief. One potential complication that arises in relation to the Bankers Trust order and/or the Norwich Pharmacal order is that it would be requiring an institution out of the jurisdiction to provide information pursuant to a court order of the English court. A question arises as to whether there is jurisdiction in this court to do that and to serve such an order out of the jurisdiction.

45. The position in relation to that had not been definitively determined. There is a decision of Waksman J in the case of *CMOC v Persons Unknown* [2017] EWHC 3599 Comm, in which an application was sought for worldwide freezing relief against persons unknown and one of the orders that the judge made at [10] related to Bankers Trust type relief and the judge said:

> "It seems to me that, first of all, there is a good case for seeking the information in documents contained in the order which I am making in respect of the banks, because that is the critical source to discover what has happened to the money which has been paid out from the claimant's bank account in London pursuant to the alleged fraud. I am satisfied there is jurisdiction to do that under Bankers Trust v. Shapira principles , and/or CPR 25.1(1)(g) . Secondly, there still has to be a case for service out even if no positive remedy is sought against those defendants other than the information. For present purposes I am satisfied that in relation to those banks which are situate outside the EU and outside this jurisdiction, that is covered by the fact that they are a necessary and proper party to the claims which have been brought against the perpetrator defendants; and in respect of service within the EU that Article 7.2 of the recast Brussels Regulation will apply, subject to the claimants

> filling out and attaching to the claim form, Form 510 where they certify to that effect."

46. The learned judge on that occasion assumed that it would be possible to make a Bankers Trust order and serve it out of the jurisdiction on a foreign entity relying upon the necessary and proper party gateway. However, I drew the claimant's attention to another decision, which is the decision of Teare J, in *AB Bank Ltd v Abu Dhabi Commercial Bank PJSC* [2016] EWHC 2082 (Comm), which it appears Waksman J was not referred to. In that case Teare J had to consider an application to serve a claim form out of the jurisdiction where there was a foreign bank innocently mixed up in a fraud that had been perpetrated and the question was whether Norwich Pharmacal/Bankers Trust type relief was a claim for an interim remedy for the purpose of the jurisdictional gateway in paragraph 3.1.5 of Practice Direction 6B.

47. The learned judge concluded in relation to various gateways, first of all, that it was not an interim remedy under section 25.1 of the Civil Jurisdiction Judgments Act 1982 but was indeed a final remedy. Secondly, that it was not an injunction ordering an act within the jurisdiction on the facts of that case, and, thirdly, that the necessary and proper party gateway was not met either. He said:

> "29. On 8 March 2016 ADCB Dubai, through its solicitors, stated that it was willing to write to the Central Bank to seek guidance as to whether the documents might be disclosed and was willing for the Claimant to join it in submitting a joint application to the Central Bank on the issue. On 9 March the Claimant, through its solicitors, requested more details about the proposed approach, doubted that the Central Bank would entertain a request from the Claimant and said that the will to disclose must come from ADCB Dubai. On 14 March 2016 the Claimant referred to the letter of 9 March 2016 and requested a detailed response. On 18 March 2016 ADCB Dubai said that it had made a reasonable offer to seek guidance

> from the Central Bank and to submit a joint application on the issue. ADCB Dubai was willing to agree the wording of an application and hoped that the Claimant's questions had been answered. However, there was no further response and so on 4 April 2016 ADCB Dubai wrote to the Central Bank informing it of this court's order and stating that it understood that "local regulations do not permit us to take action based on an order from a foreign court" and that it could only release customer information "where we receive an order from either a local court (ie UAE based) or Central Bank of UAE." ADCB Dubai went on to say that it had been argued that its terms and conditions gave a discretion for release information to third parties but that it did not understand that "general contractual rights override regulations issued by our regulator." ADCB Dubai urgently requested the Central Bank to approve its interpretation or approve the release of documents pursuant to the UK court order.
>
> 30. Counsel for the Claimant criticised the terms of the letter to the Central Bank dated 4 April 2016. I agree that it might have been better if clause 2 of ADCB Dubai's terms and conditions had been quoted and if a copy of Al Tamimi's advice had been appended. However, given the offer made by ADCB Dubai to agree the terms of any approach to the Central Bank I do not consider that ADCB Dubai can be criticised for the terms of their letter to the Central Bank.
>
> 31. On 7 April 2016 the Bank replied as follows:
>
> "While agreeing with your interpretation, you may proceed further in accordance with 2007 Treaty between UAE and UK on Mutual legal Assistance. While writing to the court, you may highlight the legal restriction on the bank to pass on any customer related information to third parties without prior approval of the Central Bank. It will therefore be necessary to follow the protocol given in the Treaty in order for the Central Bank of the UAE to pass on the required information to the court in the UK thought the proper channels."

48. He concluded in that case that there was no gateway through which the claim for Norwich Pharmacal relief could pass. He therefore set aside the order for service out of the jurisdiction.

49. Because of the potential difficulties that could possibly arise in relation to that, Mr. Connell partway through his application invited me to adjourn the Bankers Trust/Norwich Pharmacal aspect of the order. He also invited me to adjourn the aspect of the application which related to seeking a freezing

injunction. Of course, the requirements under a freezing injunction would include a risk of dissipation that might well be satisfied, he would say, in relation to the first and second defendant but he would need to address the court in relation to the position of the third and fourth defendants. Realistically, if I might say so, Mr. Connell narrowed his application before me to one for a proprietary injunction against all four defendants pending any return date at which he reserved the right to pursue the other applications.

PROPRIETARY INJUNCTION APPLICATION

50. In relation to the causes of action set out in the claim form, Mr Connell candidly recognised that it would be necessary to amend the claim form. One of the difficulties with the claim form as it was originally drafted (and I suspect that part of the reason for this was because of the application to anonymise) was that it was not as clear as it might have been precisely what causes of action were being claimed by the Insurer.

51. The potential complication is, of course, that in addition to being the Insurer, and having paid out the ransom from its own money, the Insurer was both subrogated to the rights of the Insured Customer and, secondly, there was an express assignment of such rights as the Insured Customer had. The claim form therefore raised proprietary claims in restitution and/or constructive trustees or for the tort of intimidation and/or fraud and/or conversion. It is possible that at least some of those causes of actions are those of the Insured customer, although a subrogated claim could be brought, or a claim under the assignment could be brought, by the insurer in relation to the insured customer's rights.

52. However, again Mr. Connell accepted for the purposes of today's application that the claims, in which he would seek permission to serve out of the jurisdiction and in respect of which he was seeking relief at the hearing before me, would be limited to the claims of the Insurer in restitution and/or constructive trustee against all four defendants. The rationale for that is as follows. The Insurer has paid out the sum of $950,000, that $950,000 is property belonging to the Insurer, that was used to purchase Bitcoin and the proceeds of that money can be traced into the accounts with Bitfinex, so says Mr. Connell. Those Bitcoins are being held by Bitfinex as constructive trustee on behalf of the Insurer and/or the Insurer has restitutionary claims against the third and fourth defendants who are actually holding and have possession of property which belongs to the Insurer and to which they have no right to themselves and, equally, against the first and second defendants, who are the account holders of those accounts, who have wrongfully extorted that money and have no right to the money that belongs to the Insurer.

53. I therefore turn to those causes of action. I should say that it will be necessary for the claim form to be amended, first of all, to clarify exactly what causes of action are being sought under the details of the claim and against whom. The amendments will be to make claims against the first to fourth defendants for restitution and/or as constructive trustee to recover and take a proprietary claim over those monies, including delivery up of the Bitcoins and such matters. I will discuss the precise terms of that claim form in due course with Mr. Connell, but he has indicated to me that he can give an undertaking to issue a claim form advancing those claims.

54. I therefore turn to the relief that is sought and also the relevant jurisdictional gateways.

55. Turning then to the relevant principles in relation to the granting of a proprietary injunction, the first and perhaps fundamental question that arises in relation to this claim for a proprietary injunction is whether or not in fact the Bitcoins, which are being held in this account of the second defendant with the third or fourth defendants are property at all. Prima facie there is a difficulty in treating Bitcoins and other crypto currencies as a form of property: they are neither chose in possession nor are they chose in action. They are not choses in possession because they are virtual, they are not tangible, they cannot be possessed. They are not choses in action because they do not embody any right capable of being enforced by action. That produces a difficulty because English law traditionally views property as being of only two kinds, choses in possession and choses in action. In *Colonial Bank v Whinney* [1885] 30 Ch.D 261 Fry LJ said:

> "All personal things are either in possession or action. The law knows no *tertium quid* between the two."

56. On that analysis Bitcoins and other crypto currencies could not be classified as a form of property, which would prevent them being the subject of a proprietary injunction or a freezing injunction. This exact issue has recently in November 2019 been the subject of detailed consideration by the UK Jurisdictional Task Force ("UKJT") which has published a legal statement on Crypto assets and Smart contracts, ("the Legal Statement"). The UKJT is chaired by Sir Geoffrey Vos, and Sir Antony Zacaroli is also a member. However, neither in their judicial capacity was responsible for the drafting of

the legal statement, nor have either in their judicial capacities endorsed that legal statement. Indeed Sir Geoffrey Voss explained in the foreword to the Legal Statement: "*It is not my role as a judge nor that of the UKJT or its parent, the UK Lawtech Delivery Panel, to endorse the contents of the Legal Statement*". Those responsible for drafting the Legal Statement were Laurence Akka QC, David Quest QC, Matthew Lavy and Sam Goodman.

57. It follows that the legal statement is not in fact a statement of the law. Nevertheless, in my judgment, it is relevant to consider the analysis in that Legal Statement as to the proprietary status of crypto currencies because it is a detailed and careful consideration and, as I shall come on to, I consider that that analysis as to the proprietary status of crypto currencies is compelling and for the reasons identified therein should be adopted by this court.

58. The difficulty identified in treating crypto currencies in property, as I say, starts from the premise that the English law of property recognises no forms of property other than choses in possession and choses in action. As I have already identified, crypto currencies do not sit neatly within either category. However, on a more detailed analysis I consider that it is fallacious to proceed on the basis that the English law of property recognises no forms of property other than choses in possession and choses in action. The reasons for this are set out between paragraphs 71 to 84 in the Legal Statement.

> "71. The Colonial Bank case concerned a dispute about shares deposited as security for a loan. The borrower was declared bankrupt and there was a contest for the shares between the plaintiff bank and the trustee in bankruptcy. The case was not about the scope of property generally: there was no dispute that the shares were property. The relevant question was rather whether they were things in action within the meaning of the

Bankruptcy Act 1883, an issue of statutory interpretation. If so, then they were excluded from the bankrupt estate by section 44 of that Act.

72. Lindley LJ and Cotton LJ held that the shares were not things in action. They relied principally on previous case law where the court had come to a similar conclusion in relation to the predecessor statute, the Bankruptcy Act 1869. They also drew some support from sections 50(3) and 50(5) of the 1883 Act, which appeared to make a distinction between shares and things in action.

73. Fry LJ reached the opposite conclusion, reasoning principally from what he considered to be the essential nature of a share. A share constituted "the right to receive certain benefits from a corporation, and to do certain acts as a member of that corporation" and was therefore, in his view, closely akin to a debt. He supported his conclusion by a comparison of shares to other, established, things in action, such as partnership interests and interests in funds.

74. Fry LJ's statement that "personal things" are either in possession or in action, and that there is no third category, may carry the logical implication that an intangible thing is not property if it is not a thing in action. It is not clear, however, whether Fry LJ intended that corollary and it should not in any case be regarded as part of the reasoning leading to his decision (and so binding in other cases). The question before him was whether the shares were things in action for the purpose of the Bankruptcy Act, not whether they were property, still less the scope of property generally.

75. Moreover, in making the statement Fry LJ attributed a very broad meaning to things in action. He approved a passage from Personal Property by Joshua Williams, which described things in action as a kind of residual category of property: "In modern times [sc. by the 19th century] … several species of property have sprung up which were unknown to the common law … For want of a better classification, these subjects of personal property are now usually spoken of as ... [things] in action. They are, in fact, personal property of an incorporeal nature…".

76. On appeal, the House of Lords also framed the question as one about statutory interpretation. They reversed the Court of Appeal's decision, approving the judgment and reasoning of Fry LJ. They did not explicitly address the issue of exhaustive classification between things in action and things in possession and said nothing about the definition of property. Lord Blackburn did say, however, that "in modern times lawyers have accurately or inaccurately used the phrase '[things] in action' as including all personal chattels that are not in possession". Thus, to the extent that the House of Lords agreed with Fry LJ on the classification issue, that seems to have been on the basis that the class of things in action could be extended to all intangible property (i.e. it was a residual class of all things not in possession) rather than on the basis that the class of intangible property should be restricted to rights that could be claimed or enforced by action.

77. Our view is that Colonial Bank is not therefore to be treated as limiting the scope of what kinds of things can be property in law. If anything, it shows the ability of the common law to stretch traditional definitions and concepts to adapt to new business practices (in that case the development of shares in companies).

78. Colonial Bank was referred to in Allgemeine Versicherungs-Gesellschaft Helvetia v Administrator of German Property by Slesser LJ as showing "how the two conditions of [thing] in action and [thing] in possession are antithetical and how there is nomiddle term". Again, however, the case was not about the scope of property generally but about whether something that was undoubtedly property should be classified as a thing in possession or a thing in action.

79. Most recently, Colonial Bank was cited in 2014 in Your Response v Datateam. In that case, the claimant sought to assert a lien over a database in digital form but faced the obstacle of the previous decision of the House of Lords in OBG Ltd v Allan that there could be no claim in conversion for wrongful interference with a thing in action because it could not be possessed. In an attempt to distinguish the case from OBG, the claimant argued that, even if the database could not be regarded as a physical object, it was a form of intangible property different from a thing in action and so was capable of being possessed.

80. The Court of Appeal rejected the argument. Moore-Bick LJ said that Colonial Bank made it "very difficult to accept that the common law recognises the existence of intangible property other than [things] in action (apart from patents, which are subject to statutory classification), but even if it does, the decision in OBG Ltd v Allan [2008] AC 1 prevents us from holding that property of that kind is susceptible of possession so that wrongful interference can constitute the tort of conversion." He said that there was "a powerful case for reconsidering the dichotomy between [things] in possession and [things] in action and recognising a third category of intangible property, which may also be susceptible of possession and therefore amenable to the tort of conversion" but the Court of Appeal could not do that because it was bound to follow the decision in OBG. The other members of the court agreed.

81. The Court of Appeal did not, and did not need to, go so far as to hold that intangible things other than things in action could never be property at all, only that they could not be the subject of certain remedies. The intangible thing with which they were concerned was a database, which (as Floyd LJ said) would not be regarded as property anyway because it was pure information. They did not have to consider intangible assets with the special characteristics possessed by cryptoassets.

82. In other cases, the courts have found no difficulty in treating novel kinds of intangible assets as property. Although some of those cases are concerned with the meaning of property in particular statutory contexts, there are at least two concerning property in general. In Dairy Swift v Dairywise Farms Ltd, the court held that a milk quota could be the

> subject of a trust; and in Armstrong v Winnington, the court held that an EU carbon emissions allowance could be the subject of a tracing claim as a form of "other intangible property", even though it was neither a thing in possession nor a thing in action.
>
> 83. A number of important 20th century statutes define property in terms that assume that intangible property is not limited to things in action. The Theft Act 1968, the Proceeds of Crime Act 2002, and the Fraud Act 2006 all define property as including things in action "and other intangible property". It might be said that those statutes are extending the definition of property for their own, special purposes, but they at least demonstrate that there is no conceptual difficulty in treating intangible things as property even if they may not be things in action. Moreover, the Patents Act 1977 goes further in providing, at s30, that a patent or application for a patent "is personal property (without being a thing in action)". That necessarily recognises that personal property can include things other than things in possession (which a patent clearly is not) and things in action.
>
> 84. We conclude that the fact that a cryptoasset might not be a thing in action on the narrower definition of that term does not in itself mean that it cannot be treated as property."

59. The conclusion that was expressed was that a crypto asset might not be a thing in action on a narrow definition of that term, but that does not mean that it cannot be treated as property. Essentially, and for the reasons identified in that legal statement, I consider that a crypto asset such as Bitcoin are property. They meet the four criteria set out in Lord Wilberforce's classic definition of property in *National Provincial Bank v Ainsworth* [1965] 1 AC 1175 as being definable, identifiable by third parties, capable in their nature of assumption by third parties, and having some degree of permanence. That too, was the conclusion of the Singapore International Commercial Court in *B2C2 Limited v Quoine PTC Limited* [2019] SGHC (I) 03 [142].

60. There are also two English authorities to which my attention has been drawn where crypto currencies have been treated as property, albeit that those authorities do not consider the issue in depth. They are, and I have already mentioned them, in *Vorotyntseva v Money -4 Limited t/a as Nebeus .com*, the

decision of Birss J, where he granted a worldwide freezing order in respect of a substantial quantity of Bitcoin and Ethereum, another virtual currency, and the case of *Liam David Robertson*, where Moulder J granted an asset preservation order over crypto currencies in that case.

61. In those circumstances and for the reasons I have given, as elaborated upon in the Legal Statement which I gratefully as what I consider to be an accurate statement as to the position under English law, I am satisfied for the purpose of granting an interim injunction in the form of an interim proprietary injunction that crypto currencies are a form of property capable of being the subject of a proprietary injunction.

62. I therefore turn to the applicable principles in relation to a proprietary injunction. The basis upon which proprietary injunction is sought in respect of stolen funds is summarised in McGrath Commercial Fraud in Practice, 2nd edition, at paragraph 6.247 to 6.261. As Lord Browne-Wilkinson noted in *Westdeutsche Landesbank v Islington LBC* [1996] AC 669, when property is obtained by fraud equity imposes a constructive trust on the fraudulent recipient, the property is recoverable and traceable in equity. As confirmed by Scott J in *Poly Peck International PLC v Nadir (No.2)* [1992] 4 All ER 769, the *American Cyanamid* principles apply to a proprietary injunction. First there must be a serious issue to be tried, secondly, if there is a serious issue to be tried, the court must consider whether the balance of convenience lies in granting relief sought. The balance of convenience involves consideration of the efficacy of damages as an adequate remedy, the adequacy of the cross-

undertaking as to damages, and the overall balance of convenience, including the merits of the proposed claim.

63. As I say and for the reasons I have given, I am satisfied at least to the level required for the purposes of this application for interim relief that Bitcoins constitute property. I am satisfied that the test for a proprietary injunction against each of the four defendants, is also satisfied, that there is a serious issue to be tried as between the insurer and each of the four defendants in relation to the proprietary claims which I have identified, in relation to that Bitcoin which represents the proceeds of the monies paid out by the Insurer. Clearly, the ultimate strength of the claim against each of the four defendants is not a matter for determination before me today. I am satisfied that there is at least a serious issue to be tried against all four defendants. I should say that so far as the first and second defendants are concerned, I consider that the claims are very strong because those would appear to be those defendants who in fact committed the extortion and blackmail and obtained by way of ransom the sums concerned.

64. The position is less clear in relation to the third and fourth defendants who may simply have got mixed up in another's wrongdoing but certainly they are, as I understand it, holding Bitcoin which belongs to the claimant which has (arguably) come into their possession in the furtherance of a fraud and in circumstances where they have no entitlement to retain that Bitcoin if the claimant demonstrates it is entitled to the relief which it seeks.

65. Therefore, I am satisfied that there is at least a serious issue to be tried which is all that is requited at this stage for an interim injunction. I am satisfied that

the balance of convenience lies firmly in favour of granting relief in furtherance the Insurer's claimed proprietary rights. Equally I am satisfied that damages would not be an adequate remedy in circumstances where the 96 Bitcoins could be dissipated and I am satisfied that the insurer has a strong claim to the Bitcoins in question. The relief that is being proposed is either the same or very similar to the relief I note which was granted in terms of the asset preservation order granted by Moulder J (a copy of which I have been provided with).

66. However, in addition to a proprietary injunction, there is also ancillary relief as is usual in terms of providing information so that location of assets etc and where monies have moved to, for example, can be obtained. That is particularly apposite in the case of the first and second defendants, of course, because some of the money has in fact been converted into fiat currency but, equally, it may well be the case that because of the very rapid speed at which Bitcoins could be moved, that by the time this injunction is obtained that in fact some or all of the Bitcoins may have moved from the particular exchange or the particular account within that exchange and ancillary information in relation to that is needed. I will revert to that.

67. First of all, however, I need to consider whether or not it is appropriate to grant service out of the jurisdiction in relation to the claims which are advanced. A number of gateways are relied upon under Practice Direction 6B. It is fair to say that an additional number of gateways were being considered in the context of the wider claims which I am going to adjourn, i.e. the claim for Norwich Pharmacal or Bankers Trust relief, as such, and also for a worldwide

freezing injunction. The ones which are being claimed and relied upon for the purpose of the proprietary injunction, which is the matter in relation to which relief is being sought now is, first of all (2) a claim is made for an injunction order and the defendants be prevented from doing an act within the jurisdiction; (3) a claim is made against a person upon the whom the claim form has been served or will be served otherwise in reliance on this paragraph, and (a) there is between the claimant and the defendant a real issue which it is reasonable for the court to try and (b) the claimant wishes to serve the claim form on another person who is a necessary or proper party to that claim; (5) a claim is made for an interim remedy under section 25.1 of the Civil Jurisdiction and Judgments Act 1982; (9), a claim is made in tort where damage was sustained or will be sustained within the jurisdiction, or damage which has been or will be sustained that results from an act committed or likely to have been committed within the jurisdiction.

68. In the present case, I am satisfied that the claims which are sought in terms of constructive trust and restitutionary claims, and the proprietary injunction that is sought in relation to those falls within (5), claim for interim remedy under section 25.1 of the Civil Jurisdiction and Judgments Act, as well as (9), claims in tort, where damage was sustained within the jurisdiction, the Insurer being an English insurance company who paid the money from, I am told, an English bank account and is registered here and therefore it is said has suffered loss in the money which was used to buy the Bitcoins which has ended up and has been traced through to wherever it is kept by Bitfinex.

69. I do not find it necessary to determine for present purposes whether or not the debate in relation to Bankers Trust and Norwich Pharmacal relief means that such an application - were it made - was one for interim relief or final relief because that application has been adjourned, so I express no view at the moment in relation to that.

70. So far as other gateways are concerned I consider that gateway (3) is potentially applicable because of the application of the other gateways that I have identified such that provided that any of the defendants can come within those other gateways, there are other defendants that would fall within the provisions of gateway (3). I say that also in relation to the third and fourth defendants because the relief that is being sought in terms of proprietary injunction and delivery up from them is actually substantive relief against them, i.e. the claimant is saying, "You are holding in your account Bitcoins which belonged to me, I suppose conceptually you have converted them and/or in any event that you are holding them on constructive trust for me and therefore return them." This is not simply Bankers Trust or Norwich Pharmacal type relief which is once and for all relief. There is, therefore a prospect of a trial involving all four defendants.

71. Therefore, and for the reasons I have given, I am satisfied it is appropriate to serve the claim form out of the jurisdiction in relation to the causes of action that I have identified, i.e. the restitutionary and constructive trust causes of action which will be set out in the amended claim form which I will also grant permission both for amendment and to be served out of the jurisdiction.

72. That then raises a question in relation to alternative service. The applicable principles in relation to alternative service in relation to the claim form are set out at CPR 6.15 and at 6.27 in relation to other documents. 6.15 provides: *"(1) Where it appears to the court that there is a good reason to authorise service by a method or at a place not otherwise permitted by this Part, the court may make an order permitting service by an alternative method or at an alternative place."*.

73. One difficulty, of course, arises in relation to the first and second defendants, which is that because they are persons unknown it is not as yet known what jurisdiction they are in. They could be in this jurisdiction, in which case permission to serve out would not even be needed. They could be in any jurisdiction. This is not an unknown problem and the courts have grappled with this before. Two cases in particular that spring to mind are *LJY v Persons Unknown* [2017] EWHC 3230 QB, [2018] EMLR 19, where Warby J in the context of an individual C applying for an interim non-disclosure order restraining persons unknown D from publishing allegations of serious criminal misconduct and E being alerted to the possibility of publication in an anonymous letter received from D in which D invited C to make contact with them by "an unregistered and untraceable mobile phone, in that case the court granted, an application for an order requiring C to identify themselves and to provide an address for service and B authorising C in the event of D's non-compliance with that requirement to serve the claim form by the alternative method of filing it at court.

74. Another relevant decision of Warby J's is *Clarkson plc v Persons Unknown* [2018] EWHC 417 QB, (7th March 2018). In that case company C brought proceedings for an injunction to prevent unknown person D from disclosing or using confidential information illegally obtained from C's IT systems in circumstances where D threatened to publicise the information unless a very substantial sum was paid. The court granted C an interim injunction prohibiting D from communicating or disclosing certain information to any third party or using it in any other way and made an order permitting C to serve the claim form on the email address used by D to make the blackmail threats.

75. Turning first to the first and second defendants, I consider that this is an appropriate case for alternative service. There is good reason to do so. It is not currently known where D1 and D2 are. I should say D1 and D2 are potentially one and the same person. The alternative service that is sought is as follows: that the claimant had permission to serve the order and all other documents required to be served in relation to the enforcement of the order or the proposed proceedings on the first and second defendants by email, by any address provided by the second and third defendants relating to the Bitcoin account identified at annex A, and by delivering or leaving it any physical address provided by the second and third defendants that relate to the Bitcoin account identified at annex A, and it seems to me that it would be also appropriate to authorise service of the claim form by the alternative method of filing it at court, for essentially the same reasons as were granted by Warby J in the *LJY* case.

76. So far as the third and fourth defendants are concerned, communication to date has been by email and what is sought is service by email to three email addresses, two previously used and one more recently used. I need to give more careful consideration in the case of the third and fourth defendants because they have recently communicated saying that they require to be served in the BVI and therefore the cooperative approach which they had been indicating they were going to adopt, that they could be served by email which also appears to be their normal method of service, i.e. they accept service by email (which may reflect the fact that they are indeed a technology company), they have now indicated they want to be served in person in the BVI. That does cause me some concern because they have also said in the same breath that they will cooperate with the court and any court order the court may make.

77. I consider that there are three reasons why I should make an order for alternative against the third and fourth defendants as well. The first is that this is really an urgent application. It is very important that it comes to their attention quickly because it is concerned with the 96 Bitcoins which could be dissipated at any moment. That really leads on to the second point, which is that because of the very nature of Bitcoin they can be moved at the click of the mouse and therefore steps should be taken for the proprietary injunction to come to the attention of the account at the exchange at which the Bitcoin are held at the earliest possible opportunity. Thirdly, ultimately, these Bitcoin belong to the claimant, it is a proprietary claim, and it is important that the injunction is placed as soon as possible so that their rights are preserved and the risk of that property departing to an unknown location are minimised.

78. For those reasons, and although it is exceptional to grant alternative service, I consider this is just the sort of case where there is good reason to grant alternative service and indeed even if the test is one of exceptional circumstances I am satisfied it is met for the reasons that I have identified. Therefore, I grant alternative service by email on the third and fourth defendants to the three email addresses that will be identified in the order.

79. I should say that, as is apparent, the applications before me are on a without notice basis and therefore the claimants are under a duty of full and frank disclosure. A number of matters have been raised before me orally today by Mr. Connell, as well as the matters which are set out in the supporting affidavit which I have borne well in mind, and I am not aware of any of those matters which militate against the granting of this order. I have also asked whether there are any other matters which are required to be drawn to my attention. Mr. Connell, on instructions, has told me that there are not.

80. In the usual way there is a cross-undertaking in damages which clearly is appropriate. I also have information before me which satisfied me that there is no requirement that that undertaking be fortified at least pending a return date. By the nature of the relief which I am granting in terms of the order I consider that there should be a return date within a short period of time. I will come on to the aspects of the order which deal with information but I consider a return date should be on Friday 20th December, first of all, because it seems to me that a period of about seven days is the right period for any first return date and secondly, I am conscious of the fact that after Friday it will be vacation and it will be better that if there are substantive issues arising that they are at

least either considered, or directions are given pending a further hearing, at a hearing before the end of the legal term rather than this matter appearing before a vacation judge during the course of the vacation who may not have familiarity with the case or the issues that arise. The return date will be Friday 20 December with a half day estimate.

81. The other aspect of the injunction, the proprietary injunction, is an application that information be provided both in terms of the identity and address of D3 and D4 and that applies to all four defendants, i.e. that D3 and D4 identify D1 and D2, equally D1 and D2 have to identify themselves, including their address, and any associated information that D3 and D4 may have in relation to D1 and D2. I am satisfied that that information is necessary to police the proprietary injunction that I have granted for the reasons that I have said and also I consider that the associated information would also be appropriate to be provided by way of pre-action disclosure in the action which the claimant is undertaking to commence forthwith against all four defendants. I will hear counsel in terms of the finalisation of the precise form of information to be provided.

82. In terms of timescale I can see no reason why that information should not be provided within short order. The claimant has been in correspondence with Bitfinex for some time. I have no doubt that Bitfinex has the ability to access its records and its KYC material to identify the information that is sought in relation to D1 and D2 and equally D1 and D2 clearly will know themselves that information.

83. What I am going to do is stagger the time by which the information has to be provided such that Bitfinex i.e. D3 and D4, should provide it by 4 p.m. next Wednesday, which I think is the 18th and that D1 and D2 provide the information by 4 p.m. on the 19th. I say that because until the information is supplied by D3 and D4 these proceedings may not come to the attention of D1 and D2 and so they would be unable to comply and it would be wrong in principle, it seems to me, to make the order for them to provide information at a time when it is possible the order may not have come to their attention.

84. That would mean, therefore, though, that everyone would have had to comply with the order by the return date.

85. Therefore, for the reasons I have given I am satisfied that it is an appropriate case for the granting of a proprietary injunction in the terms that I have identified against all four defendants, and for the reasons I have given, and it is appropriate to serve the amended claim form out of the jurisdiction and I give permission to do so under the gateways I have identified, together with alternative service for the reasons I have given.

86. I will adjourn the other applications for Bankers Trust/Norwich Pharmacal relief and for a worldwide freezing injunction to the return date in the first instance, no doubt in the meantime and in the light of the product of the order that has been obtained, it will be possible to give directions at that hearing as to what is to happen to those further applications. At that time, consideration can also be given, for example, in relation to orders for the provision of particulars of claim and in due course a defence so that any injunctions that are

granted will either go to trial or can be brought to fruition within a relatively short period of time. Costs reserved.

87. I will now hear counsel in relation to the finalisation of the order.

…….

Hartley M.K. West (CA Bar No. 191609)
KOBRE & KIM LLP
150 California Street, 19th Floor
San Francisco, California 94111
Hartley.West@kobrekim.com
Telephone: 415-582-4800
Facsimile: 415-582-4811

Benjamin J. Sauter (admitted *pro hac vice*)
(NY State Bar No. 4691515)
Daniel J. Saval (admitted *pro hac vice*)
(NY State Bar No. 4489514)
KOBRE & KIM LLP
800 Third Avenue
New York, New York 10022
Benjamin.Sauter@kobrekim.com
Daniel.Saval@kobrekim.com
Telephone: 212-488-1200
Facsimile: 212-488-1220

Attorneys for Foreign Representatives

UNITED STATES BANKRUPTCY COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

In re: Dooga Ltd,,	Chapter 15
Debtor in a Foreign Proceeding	Case No. 20-30157-HLB
	REDACTED ORDER GRANTING TURNOVER

Steven John Parker and Trevor John Binyon, as the foreign representatives (the "**Foreign Representatives**"), as defined in section 101(24) of Title 11 of the United States Code (the "**Bankruptcy Code**"), of Dooga Ltd. (the "**Debtor**"), debtor in a foreign proceeding (the "**U.K. Proceeding**"), as defined in Bankruptcy Code section 101(23), currently before the U.K. High Court of Justice (Proceeding No. 010642 of 2018), having filed (a) the Motion for Turnover Pursuant to Recognition Order and 11 U.S.C. §§ 542, 1507(a), 1521(a)(5) and 1521(a)(7) and Approval of Notice (the "**Motion**"); (b) the supporting Declaration of Richard Sanders and attendant exhibits; and (c) the Declaration of Steven John Parker and attendant exhibits; and no

objections or other responses having been filed thereto; and appropriate and timely notice of the filing of the Motion and the hearing thereon having been given by the Foreign Representatives; and such notice having been adequate and sufficient for all purposes; and no other or further notice being necessary or required; and after due deliberation and sufficient cause appearing therefore, the Court makes the following findings of fact and conclusions of law:

a. The Foreign Representatives may properly seek turnover of the Debtor's property within the United States pursuant to the Recognition Order entered by the Court in this proceeding (ECF No. 17) and this Court's authority under Bankruptcy Code Section 1521(a)(5). Moreover, the Foreign Representatives are also entitled to turnover relief pursuant to Bankruptcy Code Sections 542 and 1521(a)(7).

b. The contents of the Coinbase account(s) associated with Paysec principal [redacted] constitute property of the Debtor. This includes the contents and proceeds of at least the following Coinbase wallet addresses:

[redacted]

[redacted]

c. The contents and proceeds of the Bittrex account(s) associated with at least the following cryptocurrency wallets constitute property of the Debtor:

[redacted]

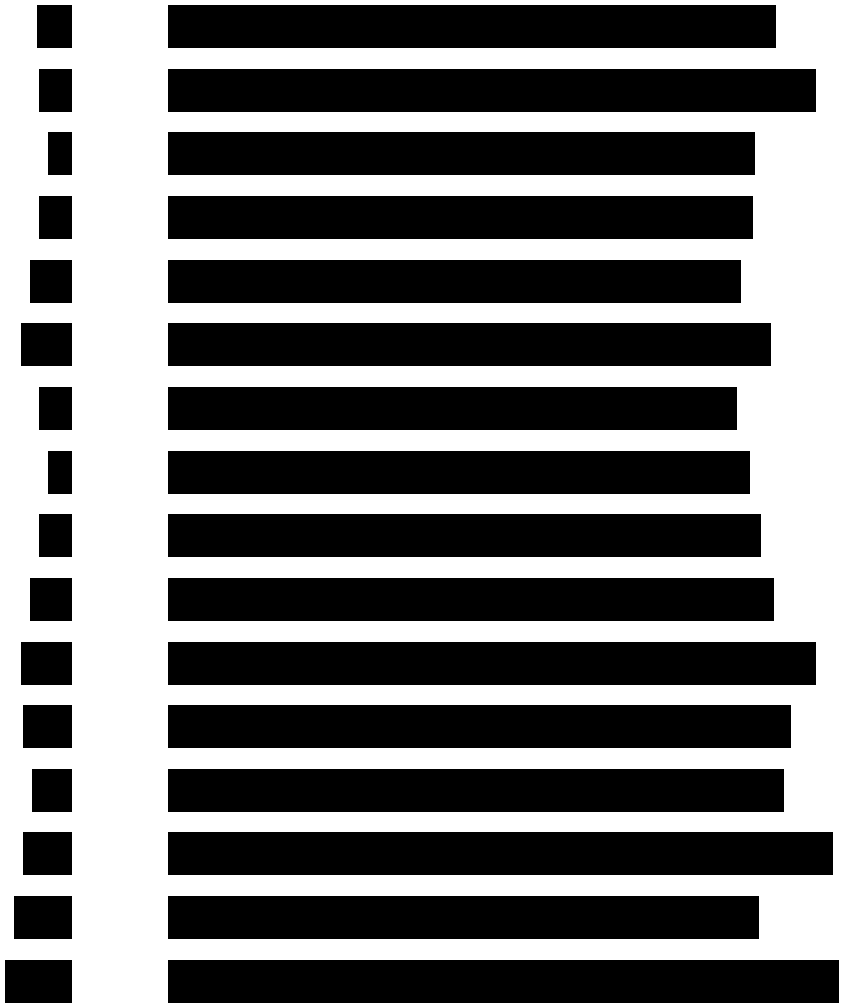
d. The Foreign Representatives have provided notice to the nominal holders of the Bittrex and Coinbase accounts by e-mailing a copy of the Motion and attendant papers to the account holders at the e-mail addresses they provided to the cryptocurrency exchanges. In addition, the Foreign Representatives have mailed copies of the Motion and attendant papers to the last known addresses of these individuals, as they were given to the cryptocurrency exchanges.

e. I conclude that such notice is reasonably calculated, under all the circumstances, to apprise the account holders of the pendency of the Motion and afford them an opportunity to present any objections, and, accordingly, that the notice provided by the Foreign Representatives constitutes good service pursuant to Fed. R. Civ. P. 4(f)(3) and, as a result, Bankruptcy Rules 7004 and 9014.

NOW, THEREFORE, IT IS HEREBY ORDERED THAT:

1. Coinbase, Inc. and all of its subsidiaries, affiliates, agents, successors, or anybody acting on its behalf are directed to turn over the contents of the account(s) associated with [redacted] to a cryptocurrency wallet or other location identified by the Foreign Representatives. This includes, if requested by the Foreign Representatives, the conversion of the contents of the subject accounts and/or wallets into another cryptocurrency or fiat currency of the Foreign Representatives' choosing. For the avoidance of doubt, this includes the contents of at least the following cryptocurrency wallets:

[redacted]



2. Bittrex Inc. and all of its subsidiaries, affiliates, agents, successors, or anybody acting on its behalf are directed to turn over the contents of the account(s) associated with [redacted] to a cryptocurrency wallet or other location identified by the Foreign Representatives. This includes, if requested by the Foreign Representatives, the conversion of the contents of the subject accounts and/or wallets into another cryptocurrency or fiat currency of the Foreign Representatives' choosing. For the avoidance of doubt, this includes the contents of at least the following cryptocurrency wallets:

3. The Foreign Representatives' provision of the Motion and attendant papers to the nominal holders of the Coinbase and Bittrex accounts by (1) e-mail to the last known e-mail address provided to the exchanges, and (2) hard copy mail to the last known address the

individuals provided to the exchanges, constitute good service pursuant to Fed. R. Civ. P. 4(f)(3), and therefore Bankruptcy Rules 7004 and 9014. Such service constitutes adequate notice of the Motion for all purposes.

4. Service of this Order shall be given by e-mail or U.S. First Class mail to (i) Coinbase; (ii) Bittrex; (iii) the United States Trustee for the Northern District of California; (iv) the Debtor; (v) all parties to litigation pending in the United States in which the Debtor is a party at the time of entry of the Order; (vi) all parties that have filed a notice of appearance in this case; and (vii) such other parties that the Court may direct, in accordance with Bankruptcy Rules 2002 and 7004(a) and (b). Service of this Order shall, additionally, be given to Dooga's creditors via the online portal maintained by the Foreign Representatives that allows creditor access to any reports, filed documents, or other updates relating to the U.K. insolvency proceedings of Dooga Ltd.

5. Service of this Order on the Coinbase and Bittrex account holders by e-mail and regular mail, as described above in Paragraph 3, shall constitute good and sufficient service of this Order and adequate notice of this Order for all purposes.

6. The terms and conditions of this Order shall be immediately effective and enforceable upon its entry.

7. This Court shall retain jurisdiction with respect to the enforcement, amendment or modification of this Order, any requests for additional relief or any adversary proceeding brought in and through this Chapter 15 case, and any request by any person or entity for relief from the provisions of this Order.

****END OF ORDER****

COURT SERVICE LIST

U.S. Trustee
Office of the U.S. Trustee (SF)
450 Golden Gate Avenue
5th Floor, Suite #05-0153
San Francisco, CA 94102

Steven John Parker and Trevor John Binyon
Opus Restructuring LLP
1 Radian Court
Knowlhill, Milton Keynes
MK5 8PJ, United Kingdom

Dooga Ltd.
c/o Opus Restructuring LLP
1 Radian Court
Knowlhill, Milton Keynes
MK5 8PJ, United Kingdom

Creditors for Dooga Ltd.
Creditor Portal: http://www.opusllp.com/opus-creditor-portal/

Coinbase Inc.
c/o Maribeth Bushey
100 Pine Street
Suite 1250
San Francisco, CA 94111
maribeth.bushey@coinbase.com

Bittrex Inc.
c/o Carolyn White
800 5th Avenue, Suite 4100
Seattle, WA 98104
cwhite@bittrex.com

Account holder #1 (name and e-mail withheld per Dkt No. 28)
58 Scholey House
3 Ingrave Street
London SW11 2SE
United Kingdom

Account holder #2 (name and e-mail withheld per Dkt No. 28)
26 Watton Lane
Water Orton
Birmingham B461PJ
United Kingdom

Account holder #3 (name and e-mail withheld per Dkt No. 28)
37 Craven Street
London WC2N 5NF
United Kingdom

IN THE HIGH COURT OF JUSTICE
BUSINESS AND PROPERTY COURTS
OF ENGLAND & WALES
COMMERCIAL COURT (QBD)

No. CL-2020-000840

Royal Courts of Justice
Strand
London, WC2A 2LL

Monday, 21 December 2020

Before:

MR JUSTICE BUTCHER

(In Private)

B E T W E E N :

(1) ION SCIENCE LIMITED — First Claimant/Applicant
(2) DUNCAN JOHNS — Second Claimant/Applicant

- and -

(1) PERSONS UNKNOWN
(being the individuals or companies, describing themselves as being or connected to 'Neo Capital', some of whom gave the aliases Marilyn Black, Claire Jones, Robert Welsh, Carey Jones, Mia Davis and Grant Ford, who participated in a scheme to induce the Applicants to transfer Bitcoins between March-October 2020 in the belief that they were investing in Dimecoin and/or Ethereum and/or Uvexo and/or Oileum)
First Defendant/Respondent

(2) BINANCE HOLDINGS LIMITED
(a company registered in the Cayman Islands)
Second Defendant/Respondent

(3) PAYMENT VENTURES INC.
(a company incorporate in the United States of America)
Third Defendant/Respondent

J U D G M E N T

(Ex Parte)

A P P E A R A N C E S

MR S. GOODMAN (instructed by Rahman Ravelli Solicitors) appeared on behalf of the Applicants.

THE DEFENDANTS / RESPONDENTS did not appear and were not represented.

_____

MR JUSTICE BUTCHER:

1 This is an urgent *ex parte* application which has been brought by the claimants for the following relief. Firstly, a proprietary injunction, a worldwide freezing order and an ancillary disclosure order against what has been called the first respondent, which are persons unknown, being individuals or companies describing themselves as being or connected to Neo Capital; secondly, a disclosure order pursuant to the *Bankers Trust* jurisdiction and/or pursuant to CPR 25.1(g) against the second and third respondents, Binance Holdings Ltd and Payment Ventures Inc; and, thirdly, permission to serve out of the jurisdiction and by alternative means. This hearing has been heard in private because of the risk of tipping off and/or that a public hearing might frustrate the object of the relief sought.

2 The claimants, in summary, believe that they have been the victims of a cryptocurrency initial coin offering or ICO fraud. By way of introduction, the first claimant is a company registered in England and Wales which specialises in gas detection products and the second claimant is an individual domiciled in England and Wales who is Ion Science's - that is to say the first claimant's - sole director and the sole shareholder of that company's holding company.

3 Over the period February to October 2020 the applicants say that they were induced by the persons unknown, who as I have said are called on this application the first respondent, who described themselves as being connected to a supposed Swiss entity called Neo Capital, to transfer £577,002 in the form of some 64.35 bitcoin in the belief that they were making investments in real cryptocurrency products. The applicants say that Neo Capital itself is not a real company. They have, they say, established that it does not appear on the Swiss version of the Companies House register, that the Swiss financial services regulator has issued a warning that it may be providing unauthorised services, and that it has no presence online beyond a website. The second respondent, Binance Holdings, is a Cayman company that the applicants say is believed to be the parent of the group of companies that operates the Binance Cryptocurrency Exchange; and the third respondent, Payment Ventures, is a US entity that it is believed is the parent of the group of companies that operates the Kraken Cryptocurrency Exchange.

4 What the applicants are seeking on this application is to secure the assets, namely the bitcoin or traceable proceeds thereof, which they believe to have been misappropriated and to preserve the assets of the Neo Capital individuals - in other words, those persons who are within what has been called the first respondent - pending enforcement; and to discover the true identity of those individuals so that an effective remedy can be sought against them.

5 The facts which have been presented on this application to me are set out in an affidavit of Syedur Rahman. I will deal with them in brief. I have read that affidavit and clearly have relied on it on this application. What is said is that in the early part of this year Mr Johns received a call from someone claiming to be from a company called Neo Capital who asked Mr Johns whether he was interested in investing in Cryptocurrency. Although Mr Johns stated that he was not, the man said that he would put Mr Johns in touch with a senior adviser at Neo Capital called Marilyn Black or Ms Black, as I will refer to her. She made contact with Mr Johns a few days later by phone and told him that she worked for Neo Capital, a company based in Zurich that specialised in investments for high net worth clients. In early March 2020 Ms Black persuaded Mr Johns to make a small personal investment into two cryptocurrencies called Ethereum and Dimecoin which are genuine cryptocurrencies. Those investments were successful, producing a return of some £15,000. The investments had been made by Ms Black herself who had convinced Mr Johns to give

her remote access to his computer. He had watched her make the trades live on the screen. The apparent success of those investments gave Mr Johns confidence in both Ms Black and services that Neo Capital could offer.

6 Subsequently, in the period between May and July 2002 Ms Black continued to grow close to Mr Johns and sought to persuade him to invest in an initial coin offering called Uvexo. She said that she had worked for Uvexo and she introduced him to a woman called Carey Jones who supposedly currently worked for Uvexo. Ms Jones told Mr Johns that Uvexo would be launching its own cryptocurrency following the ICO and that Mr Johns had the chance to buy in early and achieve a high return. Mr Johns decided that any investment in Uvexo would be made by Ion Science rather than by him personally, but Ms Black said that the investment should not be made in the company's name. What accordingly happened was that moneys were transferred from the company's account at HSBC to Mr Johns' personal account at Barclays; and the evidence is that in reliance on the implied representation that Uvexo was a genuine investment and the specific representations about Uvexo which had been made by Ms Black and by Carey Jones, Mr Johns granted Ms Black remote access to his computer. A total of £45,002 was transferred by Mr Johns from his personal bank account to his Coinbase account. That was converted into bitcoin by Ms Black and the resulting bitcoin (5.244 bitcoin) were transferred by Ms Black purportedly to a wallet address held by Uvexo.

7 Thereafter on about 3 August 2020 Ms Black called Mr Johns with a view to selling him another investment in an ICO. She then called him again and put him through to a woman called Claire Jones who described an ICO in something called Oileum which related, apparently, to a business of reclaiming muds that are a waste from drilling operations. Mr Johns was persuaded to make an investment in an ICO for Oileum and, again, Mr Johns granted Ms Black remote access to his computer. On dates between 6 and 20 August a total of £218,000 was transferred by Mr Johns from his personal bank account to his Coinbase account, that was converted by Ms Black into bitcoin (23.717 bitcoin) and those bitcoin were transferred by Ms Black supposedly into Oileum.

8 The third aspect is that in September 2020 Ms Black informed Mr Johns that the profits from Oileum amounted to some $15 million and that was now due, but that commission needed to be paid in order to release that amount. Ms Black repeatedly sought to persuade Mr Johns to make those commission payments. Ms Black persuaded Mr Johns to make payments in respect of those commissions in the following way, namely that Mr Johns again granted Ms Black remote access to his computer and between 14 and 16 September a total of £250,000 in the form of 29.083 bitcoin were transferred by Ms Black supposedly into an escrow account for commission payments.

9 The total, therefore, in summary, was that Ms Black had converted £577,000 of the funds deposited into Mr Johns's personal Coinbase account into 64.35 odd bitcoin and although £8,741 of that £577,000 was paid by way of transaction fees to Coinbase, the remainder was transferred away. Neither of the applicants have transferred any further sums, neither has been paid any part of the profits supposedly made in relation to the Oileum ICO and neither has received back any of the funds which were invested. The evidence was that Mr Johns has continued to maintain cordial contact with Ms Black, but she continues to state that the further commission payments need to be made before Oileum profits can be released.

10 I have also read as part of the application an expert report of Marlon Pinto for which I give formal permission. He is an expert in relation to cryptocurrency frauds and he gives evidence that a substantial part of the bitcoin to which I have referred as having been transferred or their traceable proceeds appears to have ended up at accounts held by the

Binance and Kraken exchanges. Mr Pinto gives evidence that the exchanges are likely to hold information about the customers to whom those accounts belong.

11 That being a summary of the evidence which has been put before me in relation to the facts, I turn to the basis in law on which this application is made. There are two preliminary matters which should be dealt with. First of all, I am satisfied that there is at least a serious issue to be tried that cryptoassets such as bitcoin are property within the common law definition of that term. There are a number of decisions, albeit on interim applications, which have come to that view, those being based, at least in part, on the analysis in the UK Jurisdiction Task Force statement on Cryptoassets and Smart Contracts. It is also right to mention that the same conclusion was reached in New Zealand in the case of *Ruscoe v Cryptopia Ltd (in liquidation)* [2020] NZHC 782. The other aspect is that there have been a number of cases which have recognised that it is possible for the court to issue claims and to make injunctions against persons unknown, the critical feature being that the description used must be sufficiently certain as to identify both those who are included and those who are not.

12 The first substantive issue which requires consideration is as to whether there is jurisdiction over the first defendant / respondent; in other words, the persons unknown. Of course, the applicants do not know where the individuals are located. They are, accordingly, seeking permission to serve them out of the jurisdiction on the basis that some or all of those individuals may neither be present nor domiciled in England and Wales. In order to obtain leave to serve out, the court has to be satisfied that there is a serious issue to be tried on the merits, that there is a good arguable case that the claims fall within one of the gateways under CPR PD 6B, and that England is the appropriate forum for the trial of the dispute.

13 As to the first of those, whether there is a serious issue to be tried on the merits, I am satisfied that the applicants can show at least a serious issue to be tried on the merits of their claims, those claims being brought or intimated in deceit, unlawful means conspiracy and by way of an equitable proprietary claim. As to the first of those, deceit, it is important to consider at the outset the question of what would be the governing law of the claim. I am satisfied that there is at least a serious issue to be tried that it is English law pursuant to Article 4.1 of Rome II on the basis that England was the place where the damage occurred, either on the simple basis that the bank account which funded the Coinbase account was an English account or that the asset was taken from the claimants' control in England and Wales, because Mr Johns granted remote access to his computer which was in England and Wales; or alternatively because the relevant bitcoin were located in England and Wales prior to the transfer. The second of those aspects is on the basis that the *lex situs* of a cryptoasset is the place where the person or company who owns it is domiciled. That is an analysis which is supported by Professor Andrew Dickinson in his book **Cryptocurrencies in Public and Private Law** at para.5.108. There is apparently no decided case in relation to the *lex situs* for a cryptoasset. Nevertheless, I am satisfied that there is at least a serious issue to be tried that that is the correct analysis.

14 As to the elements of a claim in deceit, I am satisfied that there is a serious issue to be tried that the relevant defendant, the first respondent, as they have been called, made representations which were false, which they knew were untrue or were reckless as to their truth, intending that those representations would induce the claimants and which did in fact induce the claimants to act by way of making or allowing the payments to be made, as a result of which the claimants suffered loss. I am also satisfied that there is a serious issue to be tried that the claimants have a claim in unlawful means conspiracy; and that there is a serious issue to be tried as to an equitable proprietary claim in respect of the bitcoin which were transferred on the basis that the property was obtained by fraud and was held on trust

for the victim of the fraud, or on the basis that there was a Quistclose trust in that the moneys were paid for a specific purpose which has failed. The transferors were, at least on the basis of the material which has been put before me, told that the moneys to be paid would be held and applied for a specific purpose only and the relevant sums were transferred on that basis. I also consider that in relation to the question of the availability of a gateway within PD 6B that the applicants can show a good arguable case that the tort claims fall within Gateway 9 as either the damage was sustained within the jurisdiction or was sustained as a result of acts committed within the jurisdiction, namely the making of representations to Mr Johns, the transfer of funds and the granting of remote access to Mr Johns' computer in England.

15 The equitable proprietary claim can be said to fall within Gateway 15 as being a claim made against the defendant as constructive trustee or as trustee of a resulting trust where the claim arises out of acts committed or events occurring within the jurisdiction or relates to assets within the jurisdiction, the relevant acts on this basis occurring within the jurisdiction, namely the making of or the reliance on representations and the transfer of funds or the granting of access to Mr Johns's computer, and the claim relates to assets which, on the basis of the argument which I have mentioned, have their *lex situs* within the jurisdiction.

16 Finally in relation to the proper forum, in a case of a persons unknown claim it is obviously difficult to identify another forum, but here in addition to that simple point that the claimants are domiciled in England and Wales, the relevant funds were transferred from England and Wales, the relevant bitcoin are or certainly were located in England and Wales and also the documents are in English and the witnesses are based in England, at least on the claimants' side. For all of those reasons, I am satisfied for the purposes of this application that it has been shown that England is the proper forum for the trial of the claimants' claims.

17 As to the claim for a proprietary injunction against the first respondent, the persons unknown, a proprietary injunction requires the claimant to show that there is a serious issue to be tried. That, I am satisfied, has been shown on the basis of the facts which I have already summarised. It requires the showing of a balance of convenience in favour of the grant of an injunction which, of course, involves a consideration of whether damages are an adequate remedy. Here, it seems to me, on the material I have at the moment, that the balance of convenience is in favour of granting an injunction, given that there is a *prima facie* case of wrongdoing and that there is no evidence that the individuals in question will be able to satisfy a monetary judgment for what is a significant sum. Thirdly, such an injunction involves a consideration of whether it is just and convenient to grant the order, and in this case I consider that it is on the basis of the material which is before me as it appears that the applicants have been the victims of an extensive cyber fraud.

18 The applicants also seek a worldwide freezing order and an ancillary disclosure order against the first respondent, the persons unknown. That requires that the court have jurisdiction, which I have already dealt with, and that the claimants have a good arguable case on the merits. I have already dealt with the facts. It appears to me that they do indicate a good arguable case on the merits. It is also necessary that there is a real risk of dissipation. Here I consider that the material before me indicates that there is a real risk of dissipation, given the nature of the underlying claim; the defendants' conduct which involves, if the claimants' evidence is accurate, the use of aliases and apparently false documents; and thirdly, the nature of Neo Capital which is not a registered entity and is on a regulator's warning list. There is in this case, unlike the ordinary case, no showing that there are assets which could be caught by the order. That is a typical feature of a persons unknown case. Nevertheless, it does not seem to me that it can be a bar to the grant of this type of freezing order in this type of case. Finally, the grant of a worldwide freezing order of this sort

requires that it should be just and convenient to grant the injunction and I am satisfied that it is in order to assist the victims of what appears to have been a significant and prolonged cyber fraud. Accordingly, I am willing to make the orders for proprietary injunctions and a worldwide freezing order and an ancillary disclosure order against the first respondents.

19 I turn then to the orders sought against the second and third respondents, Binance Holdings and Payment Ventures. What is sought here is disclosure orders pursuant to the *Bankers Trust* jurisdiction and/or CPR 25.1(g). This is an aspect on which the claimants place considerable importance in that they say that without such an order the true identity of the individuals who they contend were involved in this fraud may never be known, such that they would be left without any effective remedy. Mr Goodman submits that it would be highly inconvenient in a case like this if there were not the ability to obtain relief of the sort which the claimants are seeking against the exchanges in this case. I have been satisfied that there is a basis on which the court can permit service out of a claim for a *Bankers Trust* order on a party outside the jurisdiction, even where no positive remedy is sought against that respondent other than information. I have been satisfied of that to the extent of a good arguable case. The basis on which I have been satisfied is that there is a good arguable case that such respondents would be necessary or proper parties within the meaning of CPR PD 6B para.3.13 to the anchor claim. The way in which that was put and which I accept gives rise to a good arguable case is that the test for whether a party is a necessary or proper party is that established a long time ago in *Massey v Haynes* [1888] 21 QBD 330, namely if one supposes that both parties had been within the jurisdiction, would they both have been proper parties to the action? The question, therefore, is whether a claim for a *Bankers Trust* order could be brought in the same proceedings as the anchor claim. That depends on CPR 7.3 which permits the commencement of more than one claim in a claim form if they can be conveniently disposed of in the same proceedings. Here a claim for disclosure pursuant to a *Bankers Trust* order could be conveniently disposed of in the same proceedings and, indeed, it would be just and convenient in many cases, of which this would be one, for that to be the case in order to facilitate the identification of the persons unknown.

20 It is accepted by the claimants that there is authority in the form of the decision in *AB Bank Ltd v Abu Dhabi Commercial Bank PJSC* [2016] EWHC 2082, which is a case involving *Norwich Pharmacal* orders, that there was no gateway which permitted service out of the jurisdiction against a third party for the purposes of a *Norwich Pharmacal* order. The claimants contend that that decision was wrongly decided on the basis that the judge considered that it was necessary for the third party to be liable in respect of the same cause of action. That, the claimants say, was ill-founded, and that there was no necessity for that for the purposes of a party being a necessary or proper party. It is said by the claimants that the judge in the *AB Bank* case was wrong not to follow the decision in *Lockton v Google Inc* [2009] EWHC 3243 (QB) in which Eady J permitted service out of the jurisdiction of a *Norwich Pharmacal* claim.

21 I am not going on this interim application in circumstances where I have only heard one side of the argument to express a view as to whether the case of *AB Bank Ltd* was correctly decided. It seems to me that it is distinguishable on the basis that it related to *Norwich Pharmacal* orders, whereas what is here sought is a *Bankers Trust* order and on the basis that in *MacKinnon v Donaldson, Lufkin and Jenrette Securities Corporation* [1986] Ch 482 what was envisaged was that a *Bankers Trust* order might be one where there can be service out of the jurisdiction in exceptional circumstances, and that those exceptional circumstances might include cases of hot pursuit. That is this type of case. As I say, I consider that there is a good arguable case that there is a head of jurisdiction under the necessary or proper party gateway. I should also say that it seems to me that there is a good arguable case that the *Bankers Trust* case can be said to relate wholly or principally to

property within the jurisdiction on the basis of the argument which I have already identified which is that the bitcoin are or were here and that the *lex situs* is where the owner resides or is domiciled. Accordingly, I consider that there is a basis on which jurisdiction can be established.

22 The test for relief in relation to a *Bankers Trust* order is whether there have been shown to be good grounds for concluding that the property in respect of which disclosure is sought belongs to the claimant; that there is a real prospect that the information sought will lead to the location or preservation of those assets; that the order should not be wider than necessary; that the interests of the applicant in getting an order have to be balanced against any detriment to the respondent; and the applicant should provide undertakings only to use the documents for the purpose specified and, of course, to pay the respondent's expenses of compliance and to compensate the respondent for loss if the order was wrongly made. Here, as I have already said, there are grounds for concluding that the assets, the bitcoin, are the applicants' property and that there is a real prospect that the information sought from Binance Holdings and Payment Ventures will lead to the location and preservation of the applicants' property. I have already referred to the expert report of Marlon Pinto and I have already said that in fact the applicants say that the order which they seek here is really their only hope of locating and preserving the property in question. At least, they say, the disclosure will enable them to learn who received the property.

23 The question of whether the order goes wider than necessary is one which can be dealt with by looking at the terms of the order more precisely. In relation to the question of whether the interests of the applicants in getting the order outweigh the detriment to the respondents, the interests of the applicants here in obtaining the order are clear. As to detriment to the respondents, those are likely to be limited to the costs and the intrusion into the confidentiality of the identities of the alleged wrongdoers and possibly of innocent third parties. As to the first of those, costs, an undertaking will be given by the claimants. In relation to an intrusion into privacy or confidentiality, the report of Mr Pinto concludes that it is extremely unlikely that the relevant bitcoin have passed through the hands of innocent parties on the way to the Binance and Kraken exchanges, but if there is information revealed in relation to innocent parties, it will be protected by undertakings as to the use of documents. Accordingly, it appears to me that this is a case in which it is appropriate for there to be a *Bankers Trust* order in respect of the two exchanges.

24 The applicants also seek orders for alternative service pursuant to CPR 6.15 and 6.27 against all the respondents. Given that the United States and the Cayman Islands, which are the relevant domiciles for the second and third respondents, are signatories to the Hague Service Convention, the applicants have to show exceptional circumstances in order to obtain such an order. Here I consider that there are exceptional circumstances for essentially the same reasons as Bryan J considered that there were exceptional circumstances in the case of *AA v Persons Unknown* [2019] EWHC 3556 (Comm), namely that the application concerns urgent injunctions, given that the relevant bitcoin could be dissipated at any moment, the whole nature of bitcoin meaning that they can be moved at the click of a button, and that this claim involves a proprietary claim where it is important that the relief is obtained as soon as possible to preserve proprietary rights. Accordingly, I will give permission for there to be service by alternative means.

25 That concludes my reasons for saying that there should in principle be the orders sought. It will now be necessary to look at the terms of the orders in rather more detail.

CERTIFICATE

Opus 2 International Limited hereby certifies that the above is an accurate and complete record of the Judgment or part thereof.

Transcribed by ***Opus 2 International Limited***
Official Court Reporters and Audio Transcribers
5 New Street Square, London, EC4A 3BF
Tel: 020 7831 5627 Fax: 020 7831 7737
civil@opus2.digital

This transcript has been approved by the Judge

England and Wales High Court (Queen's Bench Division) Decisions

Neutral Citation Number: [2018] EWHC 838 (QB)
Case No: HQ18M01069

IN THE HIGH COURT OF JUSTICE
QUEEN'S BENCH DIVISION
MEDIA & COMMUNICATIONS LIST

Royal Courts of Justice
Strand, London, WC2A 2LL
17 April 2018

B e f o r e :

THE HONOURABLE MR JUSTICE NICKLIN

Between:
PML
Claimant

- and –

Person(s) Unknown (responsible for demanding money from the Claimant on 27 February 2018)
Defendant

Adam Speker (instructed by Taylor Wessing LLP) for the Claimant
The Defendant(s) did not attend and was not represented

Hearing date: 11 April 2018

HTML VERSION OF JUDGMENT APPROVED

The Honourable Mr Justice Nicklin :

1. This is another blackmail case in the Media & Communications List. PML is a UK company. In February 2018, its computers were secretly hacked and a very large quantity of data stolen. On 27 February 2018, the Defendant sent an email to three directors of the Claimant. Its terms were unsubtle and unambiguous:

> "As an Executive Director you should know that your company's servers are hacked. All the information from your servers – documents… databases, reports client's databases, private documents, internal workflow, all correspondence in fine (sic) ALL the DATA has been copied, safely hidden and well protected. Proofs of my words attached below (some files which I could not ever possibly have)…
>
> [details of a website which was hosting the stolen document was provided together with the login and password details ("the Cache Website")]
>
> I offer you a simple deal. All future business of the company depends upon this deal, as a result. You know, you have two ways:
>
> (1) To pay. I delete all the data. I'll also explain how to prevent such attacks in future to be safe and we forget about each other, forever.
>
> (2) Not to pay. And in this case, I publish all information in public. I think you will understand what happens next: the shares of the company will collapse; the company's credibility will be undermined; all contracts, documents, databases and all internal correspondence of the company – everything is going to be public. I can arrange it, no doubt. It's going to be the dead end for the reputation of your company.
>
> There are simply no other ways. I won't be looking for any private buyer who can also pay me for this information. I don't need that. I will never contact you again, because I'll delete all the information, so you either pay me or the data goes in total public access.
>
> As for guarantees, I act as a private person and money is all I interested in (sic). As soon as I receive money, I will delete the data and forget about your company, as I said, I don't care about it. So, you'll never hear from me again. I will not try to resell the data, because it's very dangerous and may end badly for me, as a result.
>
> Here are the terms:
>
> The cost is 300,000 (three hundred thousand Great British Pounds) paid via Bitcoin money system. Deadline – 2 weeks. (The term is based on life experience. It is enough time to verify that the data is really mine, hold meetings and/or consult regarding this matter (if necessary) and finally buy enough Bitcoin coins). In 2 weeks time, if I won't receive the money (sic) I post the data in public access (available for anyone in the world), as it is written below. I can't accept a delay if there's no VERY reasonable cause.
>
> P.S.
>
> 1) Please do not try to close the server with the data, it's just a mirror, as a proxy, it will not help you. Data is securely archived, hidden and protected.
>
> 2) Please do not make any noise; any appeal to the police, the Europol or anything else will cause an immediate publication of ALL the Information.
>
> I will explain how it will look like.

> [details are given of how the Defendant threatened to release the Claimant's data via various forums and portals, week by week]
>
> 3) So, please, do not pretend that I do not exist, do not ignore me or break the deadlines. It will simply cause the publication of all the information. You will also incur huge losses and I will go further.
>
> 4) Nothing personal – just business…
>
> Best regards. [name redacted]"

2. The email attached a selection of different documents which appeared to have come from the Claimant's computer systems. The Claimant's investigations established that someone had hacked into the Claimant's servers and extracted information and data. The threat in the email appeared to be genuine.

3. The Claimant reported the matter to the police immediately. Their investigations are ongoing.

4. Email communications between the Claimant and the Defendant continued through early March. In summary, the Claimant had no intention of paying the sum demanded but, by requesting extensions of the deadline and assurances as to the promise to delete the data if the money was paid, kept the Defendant engaged. After the expiry of one of the revised deadlines, the Defendant increased the sum he demanded to £350,000. The Defendant also threatened to start looking for buyers for the stolen data. He did, however, offer to accept payment in instalments.

5. On 21 March 2018, the Claimant applied to the Court, without notice to the Defendant, for an interim non-disclosure order to restrain the threatened breach of confidence and for delivery-up and/or destruction of the stolen data. The application came before Bryan J as interim applications Judge. The Judge sat in private, granted the injunction and made a series of further orders including anonymising the Claimant and restricting access to the Court file ("the Injunction Order"). Bryan J gave an *extempore* judgment. He was satisfied that the requirements of s.12(3) Human Rights Act 1998 were met (i.e. that the Claimant was likely to demonstrate at trial that publication of the stolen documents would not be allowed). He was also satisfied that under s.12(2) the fact that the Claimant appeared to be a victim of blackmail and that there was a risk that, were the Defendant to be given notice of the application, he would publish the information, were compelling reasons why the Defendant had not been notified. Finally, the Judge was satisfied that the Claimant, as an apparent victim of blackmail, ought to be anonymised (***ZAM -v- CFM and TFW*** **[2013] EWHC 662 (QB)** [39]-[41] and [44] *per* Tugendhat J; ***LJY -v- Person(s) unknown*** **[2017] EWHC 3230 (QB)** [2] *per* Warby J). The injunction was granted until a return day fixed for 11 April 2018.

6. The Injunction Order was served on the Defendant at 11am on 23 March 2018 using the only method available, the email account from which he had been corresponding with the Claimant. The Defendant replied at 11.09, defiantly: "*you made [your] choice, I make my own. On Monday the information will be published. Good luck*". At 14.06 he emailed to state that he had removed the password protection on the Cache Website thereby allowing them to be accessed by any user of the Internet who had the website address. At 14.30 he stated that he intended to email customers of the Claimant on Monday (presumably having harvested their email addresses from the stolen data) and added: "*shares of your company will collapse all developments will be revealed you will be an excellent example to my next customers*".

7. Separately, having established that the Cache Website was hosted by a company in another European jurisdiction ("the European Server"), the Claimant applied for and obtained an order from a Court in that jurisdiction directed at the European Server requiring it to block access to the Cache Website ("the European Order"). This order was served on the European Server at the same time as the Injunction Order was served on the Defendant. Complying with the European Order, the European Server blocked access to the Cache Website at some point in the afternoon on 23 March 2018.

8. The following morning, the Defendant emailed the Claimant: "*why did you block the proxy. I wrote that it does not make sense all the information is kept by me. On Monday, I will send you new links…*" On 26 March 2018, the Defendant renewed his threat that he was looking for buyers for the stolen data. On 27 March 2018, he told the Claimant that he had set up another website to host the documents and that this was not password protected and said: "*Do you understand that this is the end? You have a little more time to get in touch with me and start a dialogue.*"

9. As a result of their own investigations, between 23-26 March 2018 the Claimant was able to identify further websites hosting the stolen documents. The hosting companies blocked access to the documents or deleted them following service of the Injunction Order.

10. On 27 March 2018, the Claimant became aware of postings on a financial forum which referred to the Claimant and contained links to another website hosting the documents. The relevant posts also included file names of several stolen documents. On the assumption that these postings were made by the Defendant, prima facie those actions were in breach of the Injunction Order. The Claimant served the Order on the company hosting the financial forum and the relevant posts were removed. The operators of the website hosting the documents themselves also removed them, on 29 March 2018, after being contacted by the Claimant's solicitors.

11. On 9 April 2018, the Defendant made further threats of publication of the stolen data but reduced the asking price to £100,000. By the time of the hearing on 11 April 2018, no further communication had been received from the Defendant.

Application for a continuation of the Injunction Order

12. In compliance with undertakings given to Bryan J, the Claimant issued a Claim Form on 22 March 2018. Particulars of Claim were served on 9 April 2018. On 23 March 2018, the Claimant issued an Application Notice seeking the continuation of the Injunction Order until trial. A draft of the order sought was served on 9 April 2018.

13. The Claimant seeks the continuation of the Injunction Order. I granted that application. Little has changed since the Injunction Order was granted by Bryan J. The Defendant has continued to threaten to publish the stolen data unless he is paid a substantial sum of money. Indeed, as set out in Paragraph 10 above, it appears that the Defendant has tried to publish some of the data. I am quite satisfied therefore that there is a continuing threat to publish the stolen documents in breach of confidence. Bryan J was satisfied, as I am, that the Claimant is likely to demonstrate at trial that the circumstances in which the Defendant came to be in possession of the relevant documents and information (i.e. by computer hacking) imposes an obligation of confidence on the Defendant (***Tchenguiz -v- Imerman*** **[2011] Fam 116** [69]). Unsurprisingly in the circumstances, the Defendant has not suggested that there is any public interest that could justify his threatened (or actual) publications. I am satisfied therefore that the Claimant is likely to establish at trial that publication of the stolen data should not be allowed. The Defendant's failure to deliver up or delete the stolen data (a) is a further prima facie breach of the Injunction Order; but (b) justifies the continuation of that order.

Hearing in private, anonymity and restrictions on access to the court file

14. I was satisfied that it was strictly necessary to hear the application in private pursuant to CPR Part 39.3(a), (c) and (g). There is a powerful (if not overwhelming) case that this Defendant is blackmailing the Claimant. Police investigations were underway and at the hearing I had necessarily to hear evidence and submissions relating to the activities of the Defendant and the data that was stolen. The purpose of these proceedings would have been frustrated (or at least harmed) had the hearing been conducted in public. Largely, this public judgment sets out as full an explanation as I can give of the underlying facts and the reasons for the Court's decision. That mitigates, at least in part, the derogation from the principle of open justice that the Court sitting in private represents.

15. I am also satisfied that the Claimant should continue to be anonymised in these proceedings for the same reasons as Bryan J gave (see Paragraph 5 above); the Claimant is a victim of blackmail.

16. The order restricting access to certain documents on the Court file continues to be necessary in order not to defeat the injunction and anonymity order.

Order requiring the Defendant to identify himself and an address for service and service out of the jurisdiction

17. Where a defendant in a case of threatened unlawful publication hides behind anonymity, the Court has the power to include within the injunction order a requirement that s/he identify him/herself and provide an address for service ("a self-identification order"). Once a claimant has satisfied the Court that s/he is likely to demonstrate that publication should not be allowed, that may well justify the Court making a self-identification order. Such an order is necessary if, in the event of success in the claim, the remedies to which the claimant would be entitled are to be effective. Of course, a defendant may disobey the Court's order and not comply with a self-identification order as well as the non-disclosure order. But it cannot be assumed that all defendants will choose defiance. Few defendants can remain confident that they will ultimately manage to evade identification. If they fail, punishment for contempt of court would then loom large. I have recent experience in ***NPV -v- QEL & Another*** **[2018] EWHC 703 (QB)** (another blackmail case) in which a self-identification order was made against the (anonymous) Second Defendant. The Second Defendant complied with the order and provided his name and address for service.

18. Included within the Injunction Order were provisions as to service of the Claim Form (amongst other documents required to be served). There is the potential in this case that the Defendant is resident in a country which would require the Court's permission to serve the Claim Form outside the Court's jurisdiction. The claim is for breach of confidence and the detriment would be suffered within the jurisdiction were the threatened publication to take place. The Defendant is also threatening to do an act (i.e. publication) that would take place within the jurisdiction. I am satisfied that England & Wales is the proper place in which to bring the claim and I have therefore granted the Claimant permission pursuant to CPR Part 6.37 and CPR Part 6 PD6B §3.1(21) to serve the Claim Form and other documents required to be served out of the jurisdiction should that prove to be necessary.

19. I have made further ancillary orders including service of a Defence. There is a clear risk that the Defendant will refuse to participate in the proceedings. To ensure that an interim non-disclosure order is not left in near permanent suspension, the order includes the usual direction that, in the event that the Defendant does not file a Defence, the Claimant must take steps to conclude the action whether by applying for default and/or summary judgment by a particular date, in this case by 23 May 2018.

IN THE HIGH COURT OF THE
HONG KONG SPECIAL ADMINISTRATIVE REGION
COURT OF FIRST INSTANCE

ACTION NOS 902 AND 2332 OF 2018

BETWEEN

NICO CONSTANTIJN ANTONIUS SAMARA Plaintiff

and

STIVE JEAN-PAUL DAN also known as STEVE JEAN-PAUL DAN, STIVE JEAN PAUL DAN and STEVE JEAN PAUL DAN Defendant

---

(Consolidated)

Before: Deputy High Court Judge Le Pichon in Chambers
Date of Hearing: 21 October 2019
Date of Decision: 1 November 2019

D E C I S I O N

---

1. This was the substantive hearing of (1) a renewed *Mareva* application by Nico Constantijn Antonius Samara ("the plaintiff") by summons dated 11 June 2018 ("the injunction summons") on the ground that there is evidence that justifies reconsideration or constitutes a material change of circumstances; and (2) the plaintiff's summons dated 24 April 2018 for an order to inspect and take copies of bankers records used and kept by Citibank (Hong Kong) Limited, and the defendant or Gatecoin Ltd ("Gatecoin") to provide copies of certain information and documents ("the discovery summons").

2. The injunction is sought to restrain Stive Jean-Paul Dan also known as Steve Jean-Paul Dan, Stive Jean Paul Dan and Steve Jean Paul Dan ("the defendant") from disposing of assets in Hong Kong up to a value of US$2,603,639. At the conclusion of the hearing, the Decision on both summonses was reserved which I now give.

PROCEDURAL HISTORY

3. On 20 April 2018, the plaintiff made an *ex parte* application on an urgent basis and obtained an injunction. At the subsequent *inter partes* hearing on 27 April 2018, it was discharged by Madam Recorder Yvonne Cheng SC ("the Recorder") on grounds of material non-disclosure and abuse of process. The plaintiff had failed to disclose that both the Citibank account and the Gatecoin account, being the main accounts he was seeking to target with the injunction order had already been frozen independently of any court order.

4. The plaintiff then applied for a re-grant of the injunction which was refused. As the plaintiff had given no information as to his financial means, lives in Curaçao with no assets in Hong Kong and has no Hong Kong connection, he was unable to satisfy the court that his undertaking was a meaningful one. The Recorder's Reasons for Decision ("the 2018 Decision") were handed down on 15 May 2018 to which reference should be made.

5. At the call over hearing of the injunction summons on 15 June 2018, the defendant gave an undertaking pending the determination of the injunction summons not to remove from Hong Kong any of his assets up to a value of US$2,337,279.83.

BACKGROUND

6. The relevant background to these proceedings is set out in §§4 – 10 of the 2018 Decision which I gratefully adopt. For ease of reference, they are set out below:

> " 4. The Plaintiff made an affirmation dated 20 April 2018 ("the Plaintiff's 1st Affirmation") in support of his *ex parte* application. He is a citizen of the Kingdom of Netherlands living in Curaçao. He says that he had 1,000 bitcoins ('**the Bitcoins**') and came to Hong Kong during part of June 2017 so that the Defendant could help sell the Bitcoins for him, for a 3% commission.
>
> 5. As the Plaintiff (being a non-resident) could not open a Hong Kong bank account to handle the sale proceeds, he agreed that they should be deposited into the Defendant's account in Hong Kong with Citibank, from whence the funds would be transferred to the Plaintiff's bank account in Germany. The Defendant gave the Plaintiff access to the Citibank account by providing him with the login details and security token. The Plaintiff could then make transfers of funds to his account in Germany.
>
> 6. The Plaintiff says that between June and September 2017 some of the Bitcoins were traded. A main way in which this was done was through the Defendant's nominated bitcoin wallet at Gatecoin. The Plaintiff transferred some bitcoins from his personal bitcoin wallets into the Defendant's bitcoin wallet at Gatecoin so that they could be traded by the Defendant. The agreed arrangement was that the proceeds of sale would be transferred to the Citibank account.
>
> 7. The Plaintiff says that the total amount payable by the Defendant to him for the trading of the Bitcoins was US$3,118,139. Between 3 July 2017 and 6th September 2017, the Plaintiff transferred US$520,500 from the Defendant's Citibank account to his bank account in Germany.
>
> 8. The Plaintiff says that from around 14 September 2017, he noticed that the money in the Citibank account had been placed on time deposits and could not be transferred. From around the beginning of November 2017, the Plaintiff has been unable to gain online access to the account at all. The Plaintiff says that the Defendant therefore owes him US$2,597,639.

> 9. The Plaintiff says that he has not been able to locate or communicate with the Defendant since 27 or 28 October 2017.
>
> 10. In February 2018, the Plaintiff contacted Gatecoin to notify it of his concerns regarding the Defendant and to ask that Gatecoin block the Defendant from accessing his Gatecoin account. On 23 February 2018, the Plaintiff was informed by Aurelien Menant, the CEO of Gatecoin, that 40 bitcoins remained in the Defendant's Gatecoin wallet. Mr Menant agreed to block the Defendant from withdrawing the bitcoins from the wallet, but said that he would need a legal basis to block the account for any extended period of time."

THE PLAINTIFF'S RENEWED APPLICATION

7. To justify the plaintiff's renewed application, the plaintiff's counsel, Ms Seto, relied on the following 'new' evidence:

(a) An official certificate issued by the relevant French authorities, recording a decision of 21 April 2018 of the registrar of births, marriages and deaths that the defendant is called "Steve, Jacob, DAN".

(b) Evidence from the defendant's former assistant to the effect that he had been told by the defendant that the defendant had recently acquired a new passport[1] under yet a different name[2] "Stephane Jean-jacque Dan".

(c) Citibank: (i) an apologia from the plaintiff[3] to address the adverse comments made in the 2018 Decision to show that the underlying assumption he had made that the account had been blocked was not an established fact; (ii) Citibank's letter dated 16 October 2019 stating its inability to provide further information regarding the defendant's account (if any) absent a court order ordering disclosure.

---

1 The country issuing the passport was not specified.

2 There is evidence from the defendant's former wife that he has also used several other names.

3 See the plaintiff's 3rd affirmation dated 14 June 2018 ("P 3rd") §§11 – 16.

(d) Gatecoin's insolvency and the appointment of liquidators on 20 March 2019 with the plaintiff and the defendant lodging proofs of debt asserting competing proprietary claims over 45.08883 Bitcoins in the Gatecoin account.

(e) The serial number appearing on the Citibank's security token, a photograph of which is part of exhibit NCAS 6 to the plaintiff's 1st affirmation dated 20 April 2018 ("P 1st").

8. The plaintiff submitted that as the present case involves fraud, the fact that the defendant has multiple passports and names[4] is a significant factor. It was suggested that only someone who has something to hide would resort to having different identities. It was further submitted that without an injunction, the defendant will be in a position to dissipate monies in his Citibank account as well as those in the Gatecoin account in the event of any distribution by the liquidator. As the defendant is the account holder, it was said that the liquidator will likely accept his claim rather than the plaintiff's.

9. At the hearing, the defendant made no oral submissions to the effect that the court should not entertain the renewed application. It is to be noted that at the hearing before the Recorder, the court did not have to consider the substantive merits of the plaintiff's case because of issues of material non-disclosure and abuse of process. On the plaintiff's renewed application, the focus was on the defendant's objection regarding the absence of evidence of the plaintiff's ability to make good his undertaking and the absence of an offer of fortification.

---

[4] In relation to the French name change, the plaintiff initially sought to attach significance to the fact that it occurred the day after the *ex parte* injunction was granted but had to accept the established fact that the injunction was only served on the defendant on 26 April 2018: see §2 of the 2018 Decision.

THE RELEVANT LEGAL PRINCIPLES

10. It is common ground and well established that for a *Mareva* injunction to be granted, the applicant has to satisfy the court that (a) he has a good arguable case on his claim; (b) there are assets within the jurisdiction; (c) there is a real risk of dissipation of assets so as to render any judgment that may be made in his favour nugatory, and (d) the balance of convenience is in favour of grant.

WHETHER THE PLAINTIFF HAS A GOOD ARGUABLE CASE

(1) The trades

11. The plaintiff's case is that he entered into an oral agreement with the defendant in Hong Kong on 1 June 2017 who agreed to sell the plaintiff's 1,000 Bitcoins as agent in return for a commission of 3%. Between June and September 2017, the plaintiff transferred Bitcoins to the defendant for trading with, *inter alia*, Gatecoin and TD Ameritrade ("TDA").

12. The relevant evidence concerning these two accounts[5] is set out below.

(a) Gatecoin

13. The plaintiff claims to have transferred 450 Bitcoins to the defendant's nominated wallet at Gatecoin. However, he was only able to produce contemporaneous records showing the transfer of 275 Bitcoins from his Electrum wallet to the defendant's Gatecoin wallet on various dates between 8 August and 6 September 2017. The relevant transfer dates and the quantity of Bitcoins transferred are set out in §41 of P 1st. That much is common ground.

---

[5] Together they account for approximately 84% of the Bitcoins in issue.

14. It is the plaintiff's case that between July and August 2017, he had also transferred a further 175 Bitcoins to the defendant's Gatecoin wallet ("the disputed Gatecoin transfers") from another of his Bitcoin wallets but is unable to provide documentary evidence because he no longer has the Bitcoin wallet containing the relevant record "as the same has been emptied".

15. He went on to explain[6] that:

> " a bitcoin wallet can only be accessed by inserting a seed (which is a random 12-word phrase), which is only known to the owner. Thus, the ownership of the bitcoin wallet is asserted by possession of the seed. By not keeping the empty bitcoin wallet, it means that I no longer keep or remember the seed which is vital in accessing or restoring the old or empty bitcoin wallets."

16. The plaintiff acknowledged that Bitcoin transactions including those relevant to "lost" Bitcoin wallets can be traced in the public domain "by experts" but that he (the plaintiff) did not have the requisite knowledge or skills to do so.

17. Based on information that the defendant had "provided" the plaintiff between 28 July 2017 and 6 September 2017, the plaintiff set out in the table to §45 of P 1st (reproduced below) 7 trades of Bitcoins via his Gatecoin account that the defendant had facilitated:

Date	*BTC quantity*	*BTC unit price*	*Total price*	*Transaction type*
28 July 2017	25 BTC	US$ 2,683.92	US$ 67,098	OTC
31 July 2017	145.265 BTC	US$ 2,692.00	US$ 391,054	Exchange
8 August 2017	29.735 BTC	US$ 3,344.82	US$ 99,458	OTC
14 August 2017	25 BTC	US$ 3,955.15	US$ 98,878	OTC
25 August 2017	25 BTC	US$ 4,109.44	US$ 102,736	OTC / Exchange
6 September 2017	100 BTC	US$ 4,202.88	US$ 420,288	Exchange

[6] See P 1st §43.

Date	*BTC quantity*	*BTC unit price*	*Total price*	*Transaction type*
6 September 2017	100 BTC	US$ 4,491.27	US$ 449,127	OTC
Total :	450 BTC		US$ 1,628,639	

18. The 2nd and 3rd transactions listed involved the disputed Gatecoin transfers as to which the plaintiff is unable to provide documentary evidence to prove the transfers.

19. What is not known is the basis upon which the plaintiff was able to make the entries for the 2nd and 3rd transactions shown in §17 above. The plaintiff did not explain how the defendant provided the relevant information to him, what form it took and why it is no longer available.

20. For his part, the defendant does not accept the plaintiff's explanation for his inability to produce transfer records. He maintains that even if a seller's own wallets (or public/private keys) are lost, a public record of the transaction is still searchable, if he is in possession of any of the following: (1) the seller's public key to his Bitcoins wallet, (2) the buyer's public key to his Bitcoins wallet, (3) the transaction hash, (4) time, volume, quantity of the Bitcoins transacted.[7]

21. Whether Bitcoin transaction records are susceptible to public searches and, if so, how that is to be done, are not matters about which any preliminary view can usefully be formed given the state of the evidence on this issue and must be a matter for resolution at trial.

22. The issue concerning the 275 Bitcoins is different. There is no dispute that they were transferred to the defendant. The issue is

[7] See defendant's 1st affirmation dated 30 October 2018 ("D 1st") at §§17 and 20.

whether the defendant acted as principal or agent, and his rate of commission.

23. The defendant's case is that he is a Bitcoin trader who had traded with the plaintiff prior to the matters in issue in these proceedings. His relationship with the plaintiff was exclusively that of seller and buyer dealing directly with each other; all trades between them were concluded on the spot with payment being made in cash there and then or by wire transfer. However, it is noted that no mention was made of the fee/commission charged for those transactions. The defendant denied that he ever acted or agreed to act as agent for the plaintiff.

24. The defendant stated that the plaintiff approached him in 2016 wanting to sell his 1000 Bitcoins, the defendant stated he could no longer continue to trade with the plaintiff as the defendant did not have sufficient liquidity to absorb that amount of Bitcoins, "as [the plaintiff] did not wish to receive funds by bank transfer any more" [8].

25. The defendant stated that the plaintiff did not want to register or trade on soybit.com which was an online Bitcoin trading exchange the defendant started in Curaçao in November 2015. Trading on soybit.com would have required the customer/client to register on the website and provide a copy of their passport, ID and proof of address. In other words, the plaintiff wished to trade anonymously.

26. Ms Cheung, counsel for the defendant, explained that there was a price to be paid for privacy and the average commission or fee rate for OTC trades in cash for clients who wished to trade anonymously

---

[8] See D 1st at §13.

ranged from 12% to 50%. In the defendant's case, where the trade was to be anonymous, his average commission/fee rate is 40% and falls within the range.

27. The defendant referred to the website http://richfund.pe (said to be one of the largest OTC Bitcoin traders) which allegedly shows a 50% fee for conducting cash transactions in the Caribbean and Latin American region but adduced no documentary evidence in support. According to the plaintiff, the site given is defunct[9].

28. In reply, the plaintiff exhibited an article from a website reporting Bitcoin news which stated that public brokers including Richfund (whose website the defendant had relied on) and OTC's settle for a fee between 1% to 5% for which "high net worth individuals and others get privacy and security".

29. In his Consolidated Defence dated 13 March 2019 ("CD") §11(3) (reproduced below) the defendant summarised the payments he made to the plaintiff as follows:

	Date (2017)	*Bitcoin bought*	*BTC price (USD)*	*Total (USD)*	*D's fee (40%)*	*Total payout (USD)*	*Paid to P by Citibank SWIFT transfer (Transaction #)*	*Paid to P in cash (USD equivalent)*
1.	7 August	25	3,340	83,500	33,400	50,100	50,000 (8071235065)	
2.	13 August	25	3,923	98,075	39,230	58,845	50,000 (8151237626)	9,000
3.	23 August	25	4,000	100,000	40,000	60,000	50,000 (8221239538)	10,000
4.	3 September	50	4,100	205,000	82,000	123,000	50,000 (8251240538)	50,000

[9] See the plaintiff's 4th affirmation (14 December 2018) ("P 4th") at §10.

	Date (2017)	*Bitcoin bought*	*BTC price (USD)*	*Total (USD)*	*D's fee (40%)*	*Total payout (USD)*	*Paid to P by Citibank SWIFT transfer (Transaction #)*	*Paid to P in cash (USD equivalent)*
5.	4 September	50	4,230	205,000	82,000	123,000	50,000 (8311242611)	50,000
6.	5 September	50	4,230	211,500	84,600	126,900	50,000 (9051244213)	100,000
7.	6 September	50	4,230	211,500	84,600	126,900	50,000 (9061244680)	100,000
	Total :					668,745	350,000	319,000

30. What is immediately striking is that all of the SWIFT transfers were for amounts of US $50,000 each and what is even more striking is that the amounts involved all happen to be expressed in neat sums ending with three zeros.

31. It will be seen from the table that payment was said to have been effected in part by SWIFT transfers and the balance in cash at either defendant's office in Curaçao or at a location of the plaintiff's choosing[10]. Pausing there, it is to be noted that bank transfers were made to the plaintiff, despite the defendant's evidence referred to in §24 above.

32. The SWIFT transfers show the amount paid to the plaintiff and the transaction number for each of the transfers[11]. It is to be noted that for each of trades 4 and 5, when according to the defendant a sum of US $123,000 was due, only US $100,000 is shown to have been paid without accounting for the outstanding balance of US $23,000.

33. At the hearing, the court was informed that cash deliveries were made by messenger but other than the defendant's bare assertion,

---

10 CD §11(5).

11 See §§42 – 43 below.

there is no independent evidence corroborating such payments. There are also no particulars given (as to when, where and in what currency they were made) and no evidence as to how the plaintiff's instructions were communicated to the defendant.

(b) TDA

34. It is the plaintiff's case that between 27 June 2017 and 5 August 2017, the defendant acted as the plaintiff's agent in five trades totalling 387.18422 Bitcoins to TDA, a US listed brokerage firm for a total price of US $950,000. There is a supporting affirmation from Mr Sukenik who, according to the plaintiff, had brokered those transactions and provided the plaintiff with the WhatsApp messages exhibited as NCAS 32.

35. Mr Sukenik's evidence is to the effect that in his Bitcoin dealings with the defendant in June and July 2017, the defendant had represented to him that one "Nick" (ie the plaintiff) was the seller of the Bitcoins and that as brokers, the defendant and Mr Sukenik together would charge a commission fee of no more than 5% of the sales price of the plaintiff's Bitcoins sold to TDA.

36. It is common ground that 387.2 Bitcoins were transferred by the plaintiff into a co-pay account. The defendant maintained[12] that he purchased those Bitcoins and that he paid the plaintiff immediately from the Citibank account and in cash delivered to the plaintiff[13] via an employee of the defendant.

---

12 Mr Sukenik's affirmation is dated 22 February 2019 and the CD 13 March 2019.

13 See CD §12(3).

37. As pleaded in CD §12, the defendant's case is that he sold those Bitcoins to his client ("TD client") who used a TDA bank account (but who was not in any way affiliated with TDA). The defendant had asked the plaintiff to directly transfer the Bitcoins into a wallet nominated by TD client known as the co-pay wallet. TD client used a broker, Mr Sukenik, whose signature was also required by the co-pay wallet. Once the Bitcoins had been transferred into the co-pay wallet, the defendant would initiate payment and upon receipt of the payment, the plaintiff would give instructions to release the Bitcoins from the wallet.

38. A table was produced setting out the five trades with the relevant information and in particular Citibank SWIFT transfers with transaction numbers evidencing payments. It is the defendant's case that all transactions were settled by bank transfer to the plaintiff's account or/and in cash.

	Date (2017)	*Bitcoin purchased*	*BTC price (USD)*	*Total (USD)*	*D's fee (USD)*	*Total payout (USD)*	*Paid by Citibank transfer (Transaction #)*	*Paid in cash (USD equivalent)*
1.	28 June*	85.106	2,164	184,169.38	73,667.75	110,502	500 (7032068080) 10,000 (7031224133)	100,000
2.	9 July	42.553	2,350	99,999.55	39,999.82	60,000		60,000
3.	18 July	68.027	2,205	149,999.54	59,999.81	90,000		90,000
4.	25 July	97.352	2,568	249,999.94	99,999.97	150,000	10,000 (7251231017) 50,000 (8071235065)	90,000
5.	28 July	94.162	2,655	250,000.11	100,000.04	150,000	50,000 (8151237626) 50,000 (8221239538)	50,000
	Total :	387.2		934,168.52	373,667.39	560,502	170,500	390,000

*The wire transfer of the two sums of US$500 and 10,000 were initiated on 28 June 2017 but left the defendant's bank account on Monday 3 July 2017

39. The relevant extracts[14] from the WhatsApp messages in NCAS 32 exchanged on 31 July 2017 appear to relate to trades 4 and 5 and lend support to the plaintiff's case that the defendant acted as broker. Significantly, one of the messages from the defendant stated that "[the defendant], [Sukenik] and Mike[15] were all brokers in this deal"[16] and the commission involved for the brokers was no more than 5%.

(2) The Citibank transfers

40. The plaintiff's case is that as he had no Hong Kong bank account and as a visitor without a Hong Kong address and identity card he was unable to open one. In those circumstances, the defendant gave him access to the defendant's Citibank account which would be used only for the purposes of receiving the sale proceeds of the plaintiff's Bitcoins and transferring them to the plaintiff's account with the authorisation of the defendant and the defendant would not make any transfers from that account without first obtaining the plaintiff's approval[17]. On that basis, the defendant provided the plaintiff with the login details and security token.

41. The plaintiff claims to have made 11 online transfers from the defendant's account to the plaintiff's personal account in Germany between 25 July 2017 and 6 September 2017. Those transfers are set out in §30(3)(a) – (k) of the Consolidated Statement of Claim ("CSOC") and it seems they were made under the defendant's instructions[18].

42. The defendant denies ever having given the plaintiff access rights to his Citibank account. In response to §30(3) of the CSOC, the

---

14 At the court's request, a typed up version of the extracts relied on was made available.

15 "Michael" was the broker for the buyer: see message at 11:36 am.

16 This message was sent at 11:34 am, 31 July 2017 from Mr Sukenik to the defendant.

17 P 1st §38.

18 P 1st §40.

defendant dealt with those Citibank transfers by way of a table in CD §19 reproduced below:

	Transfer date (2017)	*Amount (USD)*	*Relevant trade*	*Citibank transaction reference*
(a)	25 July *	10,000	TD #4	7251231017
(b)	26 July	50,000	TD #4	8071235065
(c)	28 July	50,000	TD #5	8151237626
(d)	4 August	50,000	TD #5	8221239538
(e)	7 August	50,000	Gatecoin #1	8071235065
(f)	15 August	50,000	Gatecoin #2	8151237626
(g)	22 August	50,000	Gatecoin #3	8221239538
(h)	25 August	50,000	Gatecoin #4	8251240538
(i)	31 August	50,000	Gatecoin #5	8311242611
(j)	5 September	50,000	Gatecoin #6	9051244213
(k)	6 September	50,000	Gatecoin #7	9061244680

* additionally, on 3 July 2017, [the defendant] had transferred US$500 and 10,000 to [the plaintiff]

43. On closer consideration, an inexplicable and troubling feature emerged: three of the transaction references appears to have been used twice for different trades effected on different dates, albeit involving the same amount.

44. Take for example, the Citibank transaction reference number 8071235065. It not only evidenced a transfer made on 26 July for TD #4 but also a transfer made on 7 August for Gatecoin #1. The other transaction reference numbers used twice are 8151237626 and 8221239538.

45. There can be no rational or innocent explanation for that state of affairs. It suggests that there is something seriously awry with the evidence presented. The inference is compelling that the table was concocted to correlate with the outgoing transfers shown on the printout,

undermining the defendant's truthfulness. Necessarily, the other tables produced (§§17 and 29 above) must suffer the same fate.

(3) Absence of contemporaneous supporting evidence

46. The main criticism of the plaintiff's case of agency is that it rests on a bare assertion of an oral agreement. It was said that there is a total absence of contemporaneous material: there are no confirmatory texts, emails or other communications at the time of the trades, no account or running account of the amounts due have been produced.

47. The same criticism may be made of the defendant who has also not given supporting evidence of cash payments he made to the plaintiff which, on his own evidence, involving no less than US$669,000, made over a period of approximately two months.

48. The defendant submitted that the only piece of evidence tendered in support of trades said to have occurred is a printout of incoming and outgoing transactions of the Citibank account from 30 November 2016 to 16 October 2017 ("the printout").

49. That of course is not quite true since the WhatsApp messages exhibited are contemporaneous documents containing messages sent by the defendant at the time of the TDA trades relating to the capacity in which the defendant was acting and the rate of brokerage commission.

50. As regards the printout, it was said that the plaintiff has conducted a "reverse engineering" exercise claiming that various incoming sums are from trades and various outgoing sums were transfers of sales

proceeds made to his account. In my view, both parties have made use of the Citibank printout and indulged in a bit of "reverse engineering".

(4) Conclusion

51. As earlier noted, there is no issue over the transfer of 662.2 Bitcoins (comprising 275 Gatecoin Bitcoins and the 387.2 TDA Bitcoins) from the plaintiff to the defendant. The only questions are the amounts payable and whether they were paid.

52. As to the rate of commission, such evidence as is before the court supports the plaintiff's case. The necessary consequence is that the defendant's calculations of the amounts payable shown in the tables he has compiled cannot be believed.

53. When that is coupled with the misgivings that arise from his use of bank transaction reference numbers for wire transfers (as to which see §§42 – 45 above), and taking an overall view of the evidence, I am satisfied that the plaintiff has met the threshold of making out a good arguable case of fraud and dishonesty.

DELAY

54. By 1 November 2017, the plaintiff could no longer gain online access to the Citibank account. He made attempts but could not locate the defendant. It was not until 22 January 2018 that he sent a written demand by way of email to the defendant. He then contacted both Citibank and Gatecoin but did not make a report to the police until 18 April 2018, two days prior to his *ex parte* application.

55. That there has been some delay is undeniable but considering the material involved in the present case, the paucity of written documentation, I do not consider it inexcusable.

RISK OF DISSIPATION

56. I do not consider it appropriate to rely on the evidence of third parties (namely, the defendant's former employee and his former wife) to show that the defendant's behaviour in the past discloses an "unacceptably low standard of commercial morality". Their evidence is nothing more than hearsay from persons who may possibly entertain a grudge against the defendant.

57. However, where a good arguable case of fraud and dishonesty against a defendant has been established, the court may conclude that there is a real risk of dissipation of assets, citing *CAC Brake Co Ltd Zhuhai v Bene Manufacturing Co Ltd & Others* CACV 94/1998 (30 April 1998). I would so conclude the present case.

BALANCE OF CONVENIENCE

58. The known assets of the defendant comprise the Citibank account, any distribution by the liquidator that may be made in respect of the 45 Bitcoins in the defendant's Gatecoin account and the defendant's insurance policies with AIA International Limited.

59. At the directions hearing in June 2018, the defendant voluntarily provided an undertaking pending determination of the injunction summons. The defendant has not put forward reasons why the grant of a *Mareva* injunction which would preserve the *status quo* until trial would cause him real hardship.

60. Exhibited to P 3rd are the plaintiff's the latest available bank statements (as at the date of that affirmation) from two bank accounts which show a total balance of some €660,000. That was of course the position in June 2018 rather than what the situation is currently which may be very different. Nevertheless, one would expect that an update would have been provided to the court if any significant changes had occurred.

61. Apart from offering the usual undertaking as to damages, the plaintiff has offered to provide a fortification of such undertaking in the sum of HK$1 million to be paid into court within 14 days upon grant of an order in terms of the injunction summons.

62. The defendant submitted that, as matters stand, this amount is inadequate. Given the fact of Gatecoin's insolvency and having regard to its statement that a large part of their funds has been retained by a payment service provider, it was submitted that the liquidators are unlikely to recover those funds in full. It was said that, potentially, the defendant will stand to lose more than HK $2.52 million which, "arguably", he could have withdrawn from Gatecoin but for the injunction.

63. The Gatecoin statement gave no specifics. In any event, as the defendant himself acknowledged, whether the injunction would necessarily be the cause of that loss is "arguable".

64. Taking all relevant factors into account, I remain of the view that on the balance of convenience, the *Mareva* injunction sought should be granted.

ORDER

65. A draft order was attached to the summons. The defendant objected to the order for discovery against Citibank in (3) and Gatecoin in (4) extending to account opening documents on the ground that no explanation has been given as to why the account opening documents are relevant. The defendant's evidence is that he has had a relationship with Citibank since 2008. The plaintiff did not explain why such documents are relevant.

66. In the circumstances, there will be an order in terms save that (i) the sum of US$2,603,639 be substituted for the sum of US$2,597,639 wherever it appears, and (ii) paragraphs (3) and (4) be amended to omit any reference to account opening documents.

67. There is to be an order *nisi* of costs with certificate for counsel in favour of the plaintiff.

THE DISCOVERY SUMMONS

68. The discovery sought by this summons is against Citibank and Gatecoin who have no objection to the summons being made. At the hearing, the court intimated that the discovery summons should stand or fall with the injunction summons.

69. As the court is granting the injunction in relation to claims that are proprietary in nature, the approach must be whether the exercise of the power to order discovery is required in order to ensure that the *Mareva* jurisdiction is properly exercised and to secure its objective.

70. While the defendant has raised numerous objections to discovery on the grounds that the material sought contain confidential and commercial material involving the privacy of other individuals with whom the defendant trades and are private to the defendant in his capacity as a client of Citibank and/or Gatecoin, they would have more relevance had the discovery sought not been in the context of and in aid of a *Mareva* injunction.

71. The information is relevant to the plaintiff's proprietary claims and would reveal what has become of the Bitcoins and the fund flow of the sale proceeds. That will enable steps to be taken for their recovery. It is evident that such discovery would be in aid of the *Mareva* jurisdiction and should be granted.

72. Accordingly, there will be an order for discovery in terms of the discovery summons. There is to be an order *nisi* of costs with certificate for counsel of the discovery summons in favour of the plaintiff.

(Doreen Le Pichon)
Deputy High Court Judge

Ms Kay Seto, instructed by Hom & Associates, for the plaintiff

Ms Janine Cheung and Ms Amanda Lee, instructed by Jonathan Mok Legal, for the defendant