ONE ESSEX COURT

RECENT BITCOIN & CRYPTOCURRENCY LITIGATION

CRAIG ORR KC

Overview

- Cryptocurrency litigation landscape
- Dr Wright's claims
- Bitcoin
- Dr Wright's story
- The Identity Issue trial
- The consequentials hearing
- Conclusion

Cryptocurrency Litigation Landscape

Litigation Landscape

- To date, much cryptocurrency litigation has arisen out of fraudulent conduct:
  - Hacking / theft from cryptoasset wallets
  - Ransomware attacks
  - Other illicit use of cryptocurrency
  - Fraudulent collapse of cryptocurrency exchanges (e.g. Mt. Gox and FTX)
- Mt. Gox:
  - Japanese cryptoasset exchange handling > 70% of all Bitcoin transactions globally (early 2014).
  - Suspended trading, closed website and exchange service and filed for banktruptcy protection in February 2014.
  - Cyber hack of 850,000 Bitcoins (≈ $450m). Approx 200,000 recovered; 60,000 sold to cover bankruptcy trustee costs.
  - Distribution of balance commenced in July 2024 (≈ $8 billion at current Bitcoin price).
  - Bitcoin exchange operator (Alexander Vinnik) linked to collapse convicted in May 2024 of money laundering.
- FTX:
  - Bahamas cryptoasset exchange run by Sam Bankman-Fried (SBF) collapsed in November 2022. Third-largest exchange by volume with > 1m users.
  - Described by US prosecutors as "*one of the biggest financial frauds in American history*".
  - Gary Wang (former CTO) and Caroline Ellison (former CEO of Alameda Research) pled guilty to fraud in December 2022. SBF convicted of fraud in November 2023.

Litigation Landscape (2)

- **UK case law:**
  - Most decisions arise out of fraudulent hacking / ransomware activities. Many involve injunction applications.
  - Establish that cryptoassets are a form of property.
- **AA v Persons Unknown** [2020] 4 WLR 35 (Bryan J):
  - Claim by insurers to recover value of Bitcoins paid by their insured as ransom for a malware attack. Some Bitcoins transferred into fiat currency and balance (96) transferred to address linked to exchange (Bitfinex).
  - Insurers obtained proprietary injunction and ancillary disclosure orders against (i) hackers (persons unknown), and (ii) operators of the exchange (BVI companies).
  - Bryan J held that cryptoassets such as Bitcoin are property, despite not being choses in possession or choses in action (following report of the UK Jurisdictional Task Force chaired by Sir Geoffrey Vos).
- **Jones v Persons Unknown** [2022] EWHC 2543 (Comm):
  - Claim to recover Bitcoin from (i) operators of fake online crypto trading platform (persons unknown), (ii) owners of online wallet to which some Bitcoin had been transferred (persons unknown) and (iii) operators of the exchange hosting the wallet.
  - Worldwide freezing orders and proprietary injunction granted by HHJ Pelling QC; and summary judgment granted by Deputy Judge. Straightforward claims in deceit and unjust enrichment against the two categories of persons unknown; and exchange operators were constructive trustees as "*the controller of the wallet into which the Bitcoin was apparently paid*".
- **Osbourne v Persons Unknown** [2023] EWHC 39 (KB) (Lavender J):
  - Claim to recover two NFTs stolen by hackers from cryptoasset platform.
  - Worldwide freezing orders granted against (i) the hackers (persons unknown), and (ii) persons associated with wallets into which NFTs had been transferred (some of which were unknown).
  - Lavender J held NFTs were property, relying on **AA v Persons Unknown** and related cases.

Dr Wright’s Claims

Dr Wright's Claims

- Dr Wright claims he:
  - Wrote and published the Bitcoin White Paper ("**BWP**"), describing Bitcoin's nature and structure;
  - Wrote and released the initial versions of the Bitcoin source code ("**Bitcoin Code**").
- From 2019 onwards, these claims have generated various actions by or against Dr Wright.
- Claims by Dr Wright:
  - Claims for libel against two individuals (Peter McCormack and Magnus Granath) who had stated on twitter and elsewhere that Dr Wright was not SN and that his claims were fraudulent;
  - A claim for copyright infringement against the owner of the www.bitcoin.org website (operating under the pseudonym 'CØBRA') for hosting the BWP ("**CØBRA Claim**");
  - Claims for passing off against owners and operators of the Coinbase and Kraken cryptocurrency exchanges, on the basis that Dr Wright owned the goodwill in the term 'Bitcoin' ("**Coinbase/Kraken Claims**");
  - A claim against software developers ("**Developers**") and other entities involved in the Bitcoin ecostructure for infringing Dr Wright's copyright in the BWP and database rights in the Bitcoin blockchain ("**BTC Core Claim**").
- Claim by Crypto Open Patent Alliance ("**COPA**"):
  - Claim for (i) declarations that Dr Wright is not the author of the BWP or owner of copyright in the BWP, and (ii) injunctions restraining Dr Wright from claiming he is the author of, or owner of copyright in, the BWP and/or taking steps which involve him asserting the same.

Dr Wright's Claims (2)

- **Granath:**
  - Granath (alias 'Hodlonaut') sought, but was refused, summary judgment on the ground that Dr Wright had no realistic prospect of showing that Granath's denial of his claim to be SN caused serious harm to his reputation (**Wright v Granath** [2022] EWHC 1181 (QB))
  - Prior to Dr Wright's action, Granath had issued proceedings in Norway (where he lived) seeking a declaration of non-liability. In October 2022, the Norwegian court ruled that Granath's tweets were not unlawful (but did not actually decide whether Dr Wright was SN)
- **McCormick:**
  - McCormick (Bitcoin podcaster) originally pleaded defences of truth and publication in the public interest but abandoned those because he could not afford the costs of pursuing them to trial.
  - McCormick defended the action on the sole ground that his statements had caused Dr Wright no serious harm. This defence failed but Chamberlain J awarded Dr Wright only nominal damages on the ground that he had advanced a deliberately false case on the seriousness of harm suffered (**Wright v McCormack** [2022] EWHC 2068 (QB); upheld on appeal: [2023] EWCA Civ 892).
- **CØBRA:**
  - Proceedings served on email address of the bitcoin.org domain, but service not acknowledged. Judgment obtained by Dr Wright in default.
  - Defendant sought to challenge Dr Wright's bill of costs anonymously but Richard Smith J held disclosure of the Defendant's identity was a precondition for it participating in the proceedings, including to dispute costs. Whilst the court may for good reason protect a party's identity, it cannot entertain a situation whereby a party's identity is kept hidden *from the court* (**Wright v CØBRA** [2023] EWHC 2292 (Ch)).

Dr Wright's Claims (3)

➢ **COPA**

- COPA describes itself as a "*non-profit community of like-minded people and companies formed to encourage the adoption and advancement of cryptocurrency technologies and to remove patents as a barrier to growth and innovation*".
- Established in September 2020. Its members include cryptocurrency exchanges, such as Coinbase and Kraken, and other entities involved in the Bitcoin ecostructure.
- COPA commenced its action in April 2021, after Ontier (sols then acting for Dr Wright) had written to COPA's sols stating that he did not consent to COPA or members using the BWP and asking them to remove the BWP from their websites / social media.
- The Coinbase, Kraken and BTC Core Claims were commenced around the same time.
- Commercial issue underlying all four claims was whether Dr Wright held such IP rights in Bitcoin as enabled him to prevent its further operation without his consent. That depended on veracity of his claims to be the author of the BWP and creator of the Bitcoin system.
- Reflected divergence between adherents of different versions of Bitcoin: Bitcoin Core ("**BTC**") promoted by COPA / Developers *vs*. Bitcoin Satoshi Vision ("**BSV**") promoted by Dr Wright.
- Four actions docketed to Mellor J. In June 2023, he directed a trial of the Identity Issue, viz. ***whether Dr Wright is the pseudonymous Satsohi Nakamoto, i.e. the person who authored the BWP and created Bitcoin***.

Dr Wright's Claims (4)

- **Identity Issue**
  - Trial between Jan – March 2024. Mellor J:
    - decided that Dr Wright was not SN and that he had forged numerous documents in support of his case;
    - directed the papers be referred to the CPS to consider whether Dr Wright be prosecuted for "*wholescale perjury and forgery of documents*".
  - Trial traversed issues concerning:
    - the early history of Bitcoin;
    - the Bitcoin technology;
    - 'private proof sessions' in which Dr Wright claimed to have proved to third parties that he was SN;
    - Authenticity of documents relied upon Dr Wright to support his case.
  - Trial judgment issued on 20 May 2024 ([EWHC] 1198 (Ch)); consequentials judgment on 16 July 2024 [2024] EWHC 1809 (Ch)).
  - Mellor J did not mince words:
    - "*Dr Wright presents himself as an extremely clever person. However, in my judgment, he is not nearly as clever as he thinks he is. In both his written evidence and in days of oral evidence under cross-examination, I am entirely satisfied that Dr Wright lied to the Court extensively and repeatedly. Most of his lies related to the documents he had forged which purported to support his claim. All his lies and forged documents were in support of his biggest lie: his claim to be Satoshi Nakamoto*."
    - "*To the extent that it is said there is evidence supporting his claim, it is at best questionable or of very dubious relevance or entirely circumstantial and at worst, it is fabricated and/or based on documents I am satisfied have been forged on a grand scale by Dr Wright*."
    - "*At the same time, it is right to record that Counsel for Dr Wright put forward the best case which could possibly be presented for Dr Wright in their written and oral closing submissions, constrained as they were by the evidence I heard in this Trial*."

Bitcoin

Bitcoin

- **Bitcoin is the first decentralised cryptocurrency.**
  - Units of currency – Bitcoin - are used to store and transmit value among participants in the Bitcoin network ('nodes').
  - Bitcoin users communicate with each other using the Bitcoin protocol; available as open source software which can be run on a wide range of devices (the "**Bitcoin Code**").
  - Bitcoin are entirely virtual. The coins are implied in transactions that transfer value from sender to recipient.
  - Users of Bitcoin own digital keys that allow them to prove ownership of Bitcoin in the network. With these keys, they can sign transactions (digital messages) to unlock the value and spend it by transferring it to a new owner.
  - Keys are often stored in a digital wallet. Possession of the key that can sign a transaction is the only prerequisite to spending Bitcoin, putting the control entirely in the hands of each user.
  - Bitcoin is a distributed peer-to-peer system. There is no central server or point of control.
- **Mining:**
  - Bitcoin are created through a process of 'mining', which involves network participants (miners) competing to find solutions to a computational puzzle while processing (i.e. validating and recording) Bitcoin transactions.
  - The computational puzzle is hard to solve but the answer is easy to verify as correct, once solved. Any participant may operate as a miner, using their computer's processing power to verify and record transactions.
  - The Bitcoin Code regulates the mining function. The difficulty of the processing task that miners must perform is adjusted so that someone succeeds on average every 10 minutes. The rate at which Bitcoin are created halves every four years; and the total number of Bitcoin that will be created is fixed at 21 million. This limit will be reached by the year 2140.
  - Due to diminishing rate of issuance, Bitcoin is deflationary. It cannot be inflated by printing new money above and beyond the issuance rate. The current issuance rate (mining reward) is 3.125 Bitcoin.
  - Bitcoin mining decentralizes the currency-issuance and clearing functions of a central bank; and replaces the need for a central bank.

Bitcoin (2)

➢ **Blockchain:**

- Miners collect new transactions into blocks. Each block contains a hash of the previous block, thereby chaining the blocks together in chronological order to form the ***blockchain***.
- The contents of one block cannot be changed without changing the contents of all subsequent blocks, thereby preserving the historical integrity of the transaction ledger constituted by the blockchain.
- When creating blocks, miners validate transactions within the block by:
  - Verifying the signature on each transaction, i.e. that the sender is the current owner of the Bitcoin being remitted;
  - Checking that the Bitcoin has not been previously spent.
- Once a miner has (a) created a block of validated transactions and (b) solved the proof-of-work puzzle, it broadcasts the solution to the network, which can then verify the answer as correct and accept the newly-created block as the next addition to the blockchain.
- Miners express their acceptance of the new block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.
- Blocks have a height in the blockchain. The first block in the blockchain (at height 0) is called the *Genesis block*. This was produced on 3 January 2009 and contains a single coin generation transaction. The message used to create this transaction contains a reference to *The Times* headline on that date: "*Chancellor on brink of second bailout for banks*".

Bitcoin (3)

➢ **Digital keys:**

- Digital signatures operate with two related keys, a public and a private one. The public key can be given to anyone.
- The public and private key have an algebraic relationship. The public key is derived (by an algorithm known as 'KeyGen') from the private key. Deriving the public key from private key is easy but the opposite is cryptographically hard (i.e. impossible in practice).
- A digital signature is the digital equivalent of a handwritten signature, i.e. designed to convince others that a person / entity has signed a message. An algorithm ('Sign') allows the holder of a private key to produce a digital signature on a given message.
- Another algorithm ('Verify') allows anyone in possession of the public key to verify that a digital signature on a given message is valid, i.e. corresponds to the secret private key.
- In Bitcoin, digital signatures enable recipients of Bitcoin transfers to be satisfied that the sender was entitled to remit the relevant coins.
  - Bitcoin users typically transact using *addresses*, which are alphanumeric identifiers derived from their public key. They will often generate and use a different address every time they transact.
  - Given a Bitcoin address, a public key, a digital signature and a signed message, anyone can verify whether (i) the address was derived from the public key, and (ii) the digital signature and signed message are valid for that public key.
- Bitcoin users can therefore transfer ownership of Bitcoins they possess in a way that can be independently verified by anyone - *but does not require disclosure of the user's private key or real-word identity*.

Bitcoin (4)

➢ **Precursors to Bitcoin:**

- Prior to Bitcoin's launch in 2008/2009, others had sought to found digital currency systems but none had successfully solved the problem of avoiding double-spending without use of a central trusted authority.
  - Early 1980's: David Chaum's *digicash*
  - 1990's: Adam Back's *hashcash* and Wei Dai's *b-money*
- Promoted by the *cypherpunks*: activists who valued privacy, opposed the power of governments and sought to create social and political change through cryptography.
- Adam Back (hashcash) and Zooko Wilcox-O'Hearn (involved in digicash), who gave evidence for COPA, were members of the cypherpunk movement.
- SN's genius was to combine elements of precursor systems and concepts to create a completely decentralised digital currency system that solves the double-spend problem without relying on a central authority.
- Key innovation was to use proof of work (mining) to secure consensus about the state of transactions, on an ongoing basis.

Bitcoin (5)

- **Bitcoin launch:**
  - Events surrounding Bitcoin's launch examined closely at trial. Events not themselves controversial (generally established by email and other documents available from Satoshi Nakamoto Institute). Fundamental dispute about who was behind them, i.e. Dr Wright or someone else?

- **Key events:**
  - ***August 2008***: SN acquired the bitcoin.org domain name, which was used to establish the bitcoin.org website (subject of CØBRA Claim)
  - ***31 October 2008***: SN released BWP by posting a link on the bitcoin.org website and on the metzdowd cryptography mailing list. Abstract stated:

    "*A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trustedthird party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work.*"
  - ***3 January 2009***: SN created the Genesis block
  - ***8 January 2009***: SN uploaded the Bitcoin Code to an online platform (SourceForge) and announced its release by posting links on the metzdowd mailing list and the bitcoin.org website:

    "*I've developed a new open source P2P e-cash system called Bitcoin. Its completely decentralized, with no central server or trusted parties, because everything is based on crypto proof instead of trust. Give it a try …*"
  - ***9 January 2009***: Block 1 mined by SN
  - ***12 January 2009***: First Bitcoin transaction; transfer of 10 Bitcoin by SN from Block 9 to Hal Finney (US computer scientist)
  - ***2 May 2009***: SN corresponded with Marti Malmi (Finnish computer scientist), who thereafter helped to grow the user community
  - ***April 2011***: SN delegated responsibility for development of Bitcoin to Gavin Andresen (US computer scientist), who had been helping SN to maintain the system.

Dr Wright’s Story

Dr Wright's Story

- Dr Wright was born in Australia and lived there until 2015, when he moved to the UK.
- He claimed to have numerous master's degrees and two doctorates. He relied on his qualifications, skills and work on IT security systems in support of his case to be SN.
- From around 2009, Dr Wright was subject of investigations by the Australian Tax Office. He claimed that he had mined large amounts of Bitcoin in the early days of the system, with Dave Kleiman (US computer forensics expert) who died in 2013.
- In 2014, Dr Wright wrote to Dave Kleiman's father saying that he and Dave Kleiman were behind Bitcoin. This led to Dave Kleiman's brother, Ira Kleiman, suing Dr Wright in Florida for a share of Bitcoin allegedly mined by Dr Wright, on behalf of Dave Kleiman's estate.
- During 2015, Dr Wright was introduced by Stefan Matthews to Calvin Ayre (Canadian billionaire) and Robert MacGregor. They subsequently entered into a business arrangement whereby Dr Wright was to continue his research activities as Chief Scientist of nChain.
- In December 2015, Wired and Gizmodo (online magazines) published articles suggesting that Dr Wright was SN (but later articles questioned whether that was the case).
- Around this time, Dr Wright's offices in Australia were raided by federal police. He left Australia and settled in England.

Dr Wright's Story (2)

- After moving to England, Dr Wright took part in demonstrations (the 'private proof sessions') designed to show that he had access to private keys associated with SN:
  - **March 2016:** Dr Wright claimed to have demonstrated possession of a private key to one of the original Bitcoin blocks (generally accepted to belong to SN) to Andrew O'Hagan (journalist);
  - **March 2016:** Dr Wright claimed to have signed and verified messages using the private keys from Block 1 and 9, in a demonstration with Jon Matonis (Bitcoin Foundation founder). Mr Matonis afterwards stated that the proof was "*conclusive*" and he had "*no doubt*" that Dr Wright was SN.
  - **April 2016:** Dr Wright claimed to have demonstrated access to private keys associated with two early Bitcoin blocks, in a demonstration with Mr Andresen, who afterwards declared that he was "*convinced beyond reasonable doubt*" that Dr Wright was SN. However, following later developments (below), Mr Andresen questioned whether Dr Wright was SN. In February 2023, he posted that "*it was a mistake to trust Craig Wright as much as I did*" and expressed regret about "*getting sucked into the 'who is (or isn't) Satoshi' game*".
  - **April 2016:** Demonstrations with two journalists (Rory Cellan-Jones of the BBC and Ludwig Siegele of the Economist), during which Dr Wright claimed to have demonstrated access to the private key associated with Block 9.
- Demonstrations above were lead up to the 'Big Reveal' on 3 May 2016, when Dr Wright allegedly uploaded a post (the "**Sartre Message**") purportedly to provide 'extraordinary proof' of his identity as SN. This was subjected to serious criticism by online commentators.
- Pressure of events led Dr Wright (on his case) to self-harm by cutting his throat with a knife, resulting in his losing consciousness and being hospitalised. At around the same time, he said he destroyed a hard drive containing his private keys to early Bitcoin blocks.
- In 2019, after commencing libel proceedings against Mr McCormack and Mr Granath, Dr Wright published a blog evincing his intention to enforce his IP rights as the creator of Bitcoin.

Identity Issue Trial

Identity Issue Trial

- Main issues traversed during trial identified above (slide 10)
- **Early history of Bitcoin:**
  - Dr Wright's account of his involvement in the development and launch of Bitcoin was challenged and ultimately found to be false. According to Mellor J:

    "*Dr Wright made significant errors which Satoshi would never have made, even after this length of time. Some of these relate to Satoshi's interactions with individuals not previously made public. Others relate to technical matters which Dr Wright simply got wrong but which Satoshi would not have got wrong.*"
- **Zooko Wilcox-O'Hearn:**
  - Leading computer scientist involved in cryptography and digital currency systems for many years. Dr Wright claimed (in 2017 interview and in **McCormack** and **Granath** cases) that he had sent Bitcoin to Zooko shortly after launching Bitcoin.
  - Zooko was the first to blog about Bitcoin but had consistently said (before trial) that he never actually ran and used Bitcoin until several years later. He had been entranced by the concept when it was launched but doubted it would succeed.
  - When cross-examined at trial, Zooko described SN as his "*hero*" and said "*with some force*" (according to Mellor J) that he would certainly have remembered if he had received Bitcoin from his hero.
  - When suggested in cross-x that he became involved before 2012, he "*disarmingly*" replied: "*You underestimate my laziness and procrastination*".
  - Mellor J concluded that Dr Wright's account was "*failed guesswork*".

➢ Dr Back:

- Hotly contested issues arose between Dr Wright and Dr Back, whose hashcash system was referenced in the BWP:

  "*To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hashcash … The proof of work involves scanning for a value that when hashed, … the hash begins with a number of zero bits.*"

- Dr Wright insisted that the proof-of-work system in Bitcoin used an algorithm derived from a proof-of-work system devised by Tomas Aura, and not hashcash. He claimed that he (as SN) mentioned hashcash in the BWP because Aura had not responded to his emails whereas Dr Back did respond.
- Mellor J accepted that detailed comparison of these various methodologies may show that Bitcoin's system aligned more closely with Aura's methodology than with hashcash, but this was "*20:20 hindsight*".
- More importantly, according to Mellor J, the proof-of-work system *actually* implemented in Bitcoin did not simply look for a hash with a specified number of zeros (as per Aura's methodology and as stated in the BWP) but was more nuanced, requiring a hash which was less than a specific floating number:

  "*Dr Wright got wrong the proof-of-work system which Satoshi actually implemented in the Bitcoin Source Code, as Dr Back explained. Satoshi would not have got this point wrong.*"

- Mellor J added:

  "*In fact, there is a ready explanation as to why Dr Wright got all this wrong. It has become apparent to me that his modus operandi when pursuing his claim to be Satoshi is to do whatever he can to read and research all available materials so he is in a position to speak with authority on what happened/he did as Satoshi. This strategy is not foolproof. It comes unstuck if what Dr Wright thinks happened conflicts with (a) testimony from those who were actually involved at the time or (b) previously unpublished materials. This is yet another instance where Dr Wright has come unstuck.*"

Identity Issue Trial (3)

➢ Coding proficiency:

- The Developers mounted a sustained attack on Dr Wright's coding proficiency and understanding of the Bitcoin source code. This demonstrated (they said) that he cannot have written the source code.

- Mellor J agreed, concluding that "*a number of independent pieces of evidence … combine to present … an overwhelming case that Dr Wright did not write the Bitcoin Source Code, either by himself or with others. … his evidence that he did is fantasy*."

➢ Unsigned integer:

- Mellor J relied in particular on a "*striking passage of cross-examination*" in which Dr Wright was unable to explain the concept of an 'unsigned integer' (although it was used 294 times in the Bitcoin Code and commonly mentioned by SN in emails).

- Mellor J viewed the concept as simple; it meant an integer that is not negative.

- When taken in cross-x to a particular section of the Bitcoin Code, Dr Wright was asked by the Developers' counsel, apparently as an aside, whether he knew what 'unsigned integer' meant. When Dr Wright said that he was 'not sure how he would say it', counsel asked him to 'take a wild guess', at which point there was "*a long pause … of about 8 seconds*" before Dr Wright started to answer. According to Mellor J, this strongly contrasted "*with his usual immediate answer to any question*".

- Mellor J concluded:

> "*Bearing in mind the care, effort and skill which Satoshi used in writing the Bitcoin source code, I agree that Satoshi would not have had any difficulty in explaining the concept of an unsigned integer, even 15 years later. Accordingly, I agree with the Developers that this evidence indicates that Dr Wright did not write the Bitcoin source code.*"

Identity Issue Trial (4)

➢ Private proof sessions:

- Dr Wright said the private proof sessions he conducted were highly probative of his claim; the fact that Mr Andresen and Mr Matonis were both persuaded that he was SN was (Dr Wright submitted) highly significant. Mellor J disagreed.
- **As to Mr Matonis:**
  - Mellor J was unwilling to place much weight on Mr Matonis' endorsement of Dr Wright because he had not given evidence at trial and nothing was known about his reaction to subsequent events concerning Dr Wright's claims and whether they affected the view he had taken in March 2016.
  - Further, experts for both sides agreed that the signing session with Mr Matonis "*could very easily have been faked*".
- **As to Mr Andresen:**
  - Mr Andresen declined to assist at trial but the transcript of his evidence in the Kleiman proceedings was available.
  - Clear that Dr Wright adopted a complex process during the session with Mr Andresen, involving Dr Wright producing a signed message on his laptop; transferring the message via USB stick to a new laptop on which the Bitcoin software had been installed; downloading digital wallet software to verify the signed message; and then running that software to verify the message.
  - Considerable debate at trial about the value, utility and justification for this process.
  - Experts for both sides agreed that (i) the process adopted was not necessary to verify signature of a message with the private key relating to one of the early Bitcoin blocks; (ii) the session could have been hacked or interfered with; and (iii) this would have been relatively straightforward.
  - Dr Wright disagreed, but his evidence was not accepted. According to Mellor J:

    "*a reliable private signing could have been performed very easily and simply. Dr Wright could have signed a message on his computer, using his private key associated with the public key for block 9. That signed message could have been passed via a clean USB stick to, for example, Mr Andresen, who could then have run the Verify algorithm on his own laptop to determine if it was genuine. Nothing more complicated was required. Against that simple point (on which the experts were agreed) there is a marked contrast with the complicated and elaborate procedures which seem to have been adopted by Dr Wright*."

Identity Issue Trial (5)

➢ Forgery / authenticity of documents:

- Convoluted procedural history:
  - Dr Wright produced a list of his (107) primary reliance documents.
  - COPA served report of its forensic documents expert (Mr Madden), running to 970 pages. Concluded that all reliance documents, and many more, were inauthentic / manipulated / unreliable.
  - Dr Wright served report of his forensic documents expert (Dr Placks). Agreed that some, but not all, of reliance documents were manipulated / unreliable.
  - COPA limited to relying at trial on 50 forgery allegations.
  - Dr Wright disclosed and sought to rely upon (i) 97 documents from a newly discovered hard drive (the "**BDO Image**") and (ii) certain LaTeX files said to compile the BWP.
  - Disclosure / forensic examination of newly disclosed docs required short adjournment of start of trial. COPA limited to relying on (i) 20 original forgery allegations, and (ii) 20 forgery allegations in respect of the BDO Image documents and LaTeX files.
- By time of trial, experts for both sides agreed that (i) most original reliance docs, (ii) 71 docs from the BDO Image and (iii) the LaTeX files, were inauthentic / manipulated.
- Dr Wright's forensic document experts were not called at trial (but reports and joint statements were in evidence).
- Mellor J concluded that all forgery allegations were proved.

Identity Issue Trial (6)

➢ BDO Image:

- Dr Wright said that on 15 September 2023 (≈ 2 weeks after service of Madden's 1st report), he discovered two hard drives in a drawer at his house not previously disclosed. One of these contained an image of a drive captured on 31 October 2007, when he was at BDO.
- BDO Image was collected by e-disclosure providers on 20 September 2023.
- Dr Wright identified 97 docs on the BDO Image supporting his case; 71 were directly probative of his claim to be SN.
- Dr Wright said that he had not touched the BDO Image since 31 October 2007; it was a "*time capsule*" and the 71 docs proved his authorship of the BWP and creation of Bitcoin (e.g. drafts of BWP / sections of Bitcoin Code).

➢ However, forensic examination showed that the BDO Image was actively edited from 17-19 September 2023. Experts agreed:

- The BDO Image as a whole was not authentic. The editing in September 2023 was not result of an automated process (as Dr Wright suggested) but rather editing by a computer user which involved clock manipulation to backdate the insertion / editing of documents.
- Each of the 71 docs was manipulated / unreliable.

➢ At trial, Dr Wright said that the editing / manipulation of docs on the BDO Image must have been the result of his computer having been hacked by Christopher Ager-Hanssen, the former CEO of nChain with whom Dr Wright had fallen out by the time of trial.

➢ Mellor J rejected Dr Wright's explanation for the editing / manipulation of the BDO Image. He concluded:

- The BDO Image was seeded by Dr Wright with all 71 docs in September 2023;
- Dr Wright was responsible for the manipulations identified by the experts; the notion that a 'bad actor' was responsible for the forgeries on the BDO Image was "*literally **in**credible*" and "*completely implausible*".

Identity Issue Trial (7)

➢ LaTeX Files:

- LaTeX is a document preparation system used to ensure high quality typesetting in publications.
- In November 2023, Dr Wright disclosed certain LaTeX files which he said compiled a copy of the BWP that was 'materially identical' to the original. He blamed the late disclosure on erroneous advice from his former sols.
- The LaTeX files were hosted on Overleaf, an online platform. Dr Wright said that no metadata was available from Overleaf showing the provenance of the LaTeX files.
- Dr Wright said that it was 'practically infeasible' to reverse engineer the code in the LaTeX files from the BWP; and that his mere possession of the LaTeX files was highly probative of his authorship of the BWP.

➢ Experts for both sides agreed that:

- The LaTeX files did not compile into an identical or near identical copy of the original BWP; there were "*substantial discrepancies*";
- The original BWP was created with OpenOffice 2.4, and not LaTeX;
- LaTeX files relied upon by Dr Wright incorporated packages / commands that did not exist when the BWP was produced.

➢ Further investigation established that metadata *was* available on Overleaf, resulting in disclosure of additional LaTeX files by Dr Wright before and during trial.

- This enabled the Developers to analyse (and produce at trial animations showing) the precise editing of the LaTeX files from 17 November 2023 up until the time the files were disclosed.

Identity Issue Trial (8)

➢ In his Judgment, Mellor J:

- Analyses the nature, provenance and authenticity of the LaTeX files in great detail.
- Concludes that the LaTeX files were recent forgeries created by Dr Wright.

➢ Specifically, Mellor J found:

- The Developers' animations showed the process by which Dr Wright forged the LaTeX files in real time; they were "*the digital equivalent of a video capturing Dr Wright in the act of forgery*".
- The LaTeX files were created by Dr Wright in September 2023 as "*a key part*" of his response to Madden's 1st report; that report "*taught [Dr Wright] the pitfalls of documents containing metadata. So he pivoted to a set of documents which (he thought) either contained no metadata or much less than the documents from his original disclosure*".
- Dr Wright's application (made at the PTR) for permission to rely upon the LaTeX files was "*a fraud on the Court and a fraud on COPA and the Developers*".
- Dr Wright's "*dishonest account of the production of the [BWP] shows that Dr Wright does not know how the BWP was produced*" and that he "*is not Satoshi Nakamoto*".
- The BWP was produced in OpenOffice 2.4, as its metadata records and the experts agreed, and not LaTeX. Dr Wright's "*elaborate attempt to carve an alternative narrative by forging documents in LaTeX mark him as a fraud and his claim in these proceedings as a fraudulent claim*".

Identity Issue Trial (9)

➢ Ontier email:

- Described by Mellor J as a "*particularly outrageous forgery*" since it was "*created in the middle of trial for the purpose of trying to explain away other allegations of forgery*".

➢ Sequence of events:

- On Day 4, in the course of cross-x concerning screenshots of accounting records relating to his early mining activities, Dr Wright said that the screenshots had been taken by Ontier in 2019.
- The following day, Shoosmiths (Dr Wright's sols at trial) informed the Court, after taking instructions from Dr Wright with the Court's permission, that Ontier had informed them that the screenshots were taken in March 2020, immediately after they were given access to Dr Wright's online accounting system, and not during 2019.
- Dr Wright nevertheless insisted, in cross-x on Day 5, that he had given Ontier access to the accounting system in late 2019 and had emails in disclosure showing that to be the case.
- On the weekend after Day 5, Dr Wright's wife forwarded to Shoosmiths an email from Dr Wright to Ontier dated 2 December 2019 (on its face), recording that Dr Wright had given Ontier log-in details to his accounting system on that date (the "**Ontier Email**").
- The following week, Dr Wright re-iterated in further cross-x that he gave access details to Ontier in 2019 and had emails to prove it.
- The same day, Shoosmiths were informed by Ontier that they had received the Ontier Email (dated 2 December 2019 on its face), but only on *18 February 2024* (the date when it was forwarded by Dr Wright's wife to Shoosmiths).
- Dr Wright waived privilege over the Ontier Email and the information provided by Ontier; this material was then disclosed.

➢ Mr Madden (COPA's expert) concluded that timestamp anomalies showed that the Ontier Email was not authentic to its stated date.

Identity Issue Trial (10)

- Dr Wright disputed Madden's analysis; and said that the email received by Ontier on 18 February 2024 was spoofed by an unknown bad actor.

- Mellor J was "*entirely satisfied that the [Ontier Email] was forged by Dr Wright*". Specifically, he found:

  - The Ontier Email was created by Dr Wright manipulating a genuine email dating from 2 December 2019 whilst his computer clock was backdated.

  - The new email was then sent by Dr Wright to Ontier (on 18 February 2024) and to his wife, his intention being to deploy the email in support of his case.

  - When later stating in cross-x that he had emails showing that Ontier were given log-in details in 2019, Dr Wright was relying on emails he knew he had recently forged.

  - Dr Wright's story that a bad actor spoofed the email sent to Ontier on 18 February 2024 was "*absurd*".

- Mellor J commended the sols involved:

  "*In all of this, the responsibility for the forgery lies firmly at Dr Wright's door. No blame attaches to any of the solicitors who acted on his behalf at various times. Indeed, both Ontier and Shoosmiths behaved entirely properly and their actions enabled the forgery to be exposed.*"

Identity Issue Trial (11)

➢ **Conclusion of trial**

- On last day, following Developers' closing subs, Mellor J thanked parties for their written and oral arguments which would, he said, require him to prepare "*a fairly lengthy written judgment*" which would be handed down in due course.
- He then added:

  "*However, having considered all the evidence and submissions presented to me in this trial, I've reached the conclusion that the evidence is overwhelming. Therefore, for reasons which will be explained in that written judgment in due course, I will make certain declarations.*"

- He then declared that Dr Wright (i) was not the author of the BWP, (ii) is not SN, (iii) is not the person who created the Bitcoin system, and (iv) is not the author of the initial versions of the Bitcoin software.

Consequentials Hearing

Consequentials hearing

➢ Injunctions:

- Dr Wright did not object (in principle) to orders sought by COPA preventing him or his companies pursuing (or threatening to pursue) further proceedings in this jurisdiction or elsewhere to relitigate his claim to be SN.
- However, COPA also sought to injunct Dr Wright and his companies from:
  - *asserting* that Dr Wright possessed legal rights as SN; and/or
  - *publishing* or causing to be published statements to the effect that Dr Wright is SN, or the author of the BWP or creator of Bitcoin.
- Dr Wright argued that these additional injunctions were (a) unnecessary, (b) disproportionate and (c) contravened his right to freedom of expression under Article 10 of the ECHR.
- COPA argued that Article 10 does not protect falsehoods and was therefore not engaged in the present case; and that even if it was, the additional injunctions they sought were justified and appropriate.
- Mellor J considered the arguments on the additional injunctions to be "*more finely balanced*" and decided to "*err on the side of caution*" by not granting them (subject to COPA having permission to apply for 2 years).

Consequentials Hearing (2)

- **Dissemination orders:**
  - Dr Wright did not object to posting notice of the Court's decision on his website for 6 months but contended that further dissemination orders sought by COPA were disproportionate and unnecessary (relying on *Samsung Electronics v Apple*).
  - Mellor J decided that a website notice was not on its own adequate and directed Dr Wright also to pin a notice on his X / Twitter feed and Slack channels for 3 months.
  - However, COPA's application for an order that a half-page notice be published in The Times was rejected for being "*a somewhat vindictive response*" to Dr Wright's half-page publication in the same newspaper of an open settlement offer before trial.

- **CØBRA Claim:**
  - Mellor J set aside the default judgment obtained by Dr Wright in the CØBRA Claim, and the orders made in that action, on the ground that they were obtained in a claim which was fraudulent.
  - Power exercised pursuant to:
    - CPR 3.1(7): variation / revocation of an order;
    - CPR 13.3(1)(b): setting aside judgment in default for 'good reason';
    - Court's inherent jurisdiction.

Conclusion

Conclusion

- Resolution of Identity Issue leaves the many interesting legal issues raised by the Coinbase, Kraken and BTC Core Claims unresolved.

- Judgment is treasure trove for those interested in:
  - history and workings of Bitcoin;
  - forensic examination of digital documents.

Thank you

ONE ESSEX COURT

www.oeclaw.co.uk

London One Essex Court
Temple, London EC4Y 9AR, UK
+44 (0)20 7583 2000
clerks@oeclaw.co.uk

Singapore 28 Maxwell Road
#04-14 Maxwell Chambers Suites
Singapore 069120
+65 6634 1363
singapore@oeclaw.sg