Articles + Publications | September 15, 2022

“Trust the Process”? – Privacy and Cybersecurity Issues With Court Service of Process via NFT

Privacy & Cybersecurity Newsletter

WRITTEN BY

Tara L. Trifon | Michael Jacobs

Recently courts in New York and London granted orders in two unrelated cases – *LCX AG v 1.274M U.S. Dollar Coin*[1] and *D’Aloia v Binance Holdings & Others*[2] – authorizing the claimants to serve proceedings on anonymous defendants by way of a non-fungible token (“NFT”).

These appear to be the first known judicial decisions permitting service using NFTs, transmitted by way of “*airdrop*” into the defendants’ wallets on the Ethereum blockchain. Delivery of a token by airdrop entails the sending party transmitting a token from one wallet to another party’s wallet on the blockchain, typically on an unsolicited and unexpected basis.

This article considers the privacy and cybersecurity implications of effecting (and receiving) service via NFT in this way.

Background: NFTs

NFTs have found prominence over the last 18 months mainly as a medium for collectible digital assets, particularly digital artwork, yet there are potentially several diverse uses for the technology.

NFTs are uniquely identifiable packets of information stored on the blockchain (commonly the Ethereum blockchain network). This information may include smart contracts (which are essentially lines of code setting out the parameters of how the NFT functions) and associated media, such as text, image files, music or videos. This media information can be stored “on-chain” (i.e. as data stored on the blockchain network itself), but is more often stored “off-chain”, i.e. on the conventional worldwide web, with the on-chain token simply acting as a signpost to the relevant media file.

Various uses of NFTs and blockchain have been explored in recent years, such as: ticketing,[3] real estate title records[4] and identity verification.[5] However, NFTs and blockchain are not typically used to transmit personal or business communications. The New York and London decisions notwithstanding, it is unlikely that service of court proceedings via NFT will become the norm any time soon. Although it is now legally and technologically possible to serve proceedings by this method (subject to a court’s permission), conventional methods of service, such as post, courier or email, will likely remain the most appropriate to use for the foreseeable future.

That being said, service by NFT may have a real and practical use in litigation in a number of situations:

- For claimants who are victims of cryptoasset theft or fraud, where the identity of a defendant(s) is unknown (beyond a wallet address on the blockchain);
- When the defendant's wallet is not associated with a centralized exchange (e.g. Binance or Coinbase), such that the defendant's identity cannot be ascertained through third party disclosure orders against the exchanges.[6]
- When timing is of the essence, such as to reduce the risk of the defendant dissipating assets.
- When the defendant is located outside the claimant's jurisdiction and service by conventional means (such post or even via diplomatic channels) could take several weeks if not months.

LCX and *D'Aloia*

In *LCX* and *D'Aloia*, the claimants were the victims of cryptocurrency theft and fraud respectively. *LCX* concerned the theft of US$ 8 million of cryptocurrency from the claimant's wallet, whereas Mr D'Aloia alleged that he was the victim of a scam in which he had been induced to transfer cryptocurrency to wallets controlled by one or more unknown persons, operating under the guise of a website with the domain tda-finan.com.

In each case, the claimant commenced proceedings to recover the misappropriated cryptocurrency and applied for the court's permission to serve proceedings on the defendants via NFT (the "Service Token"). At the time of issuing proceedings, the personal identity of the defendants was not known beyond their wallet addresses (which take the form of a unique hex string of 42 characters), nor was it possible to identify the residence or place of business of the people who controlled those wallets. As such, the claimants sought permission to serve court documents by way of sending a Service Token to those wallets.

In the case of *LCX*, the Service Tokens contained a hyperlink to the claimant's lawyer's website which hosted the relevant court documents being served.[7] The hyperlinks also contained a tracking mechanism, so that it could be ascertained if the defendant clicked through to view the relevant documents. It is unclear from the reported decision of *D'Aloia* as to how the relevant documents were transmitted in that case.

Privacy Considerations

There are two aspects of blockchain technology which are fundamentally incompatible with privacy and the rights of individuals under the EU General Data Protection Regulation ("GDPR") and the Data Protection Act 2018 in the UK ("DPA"):

- Blockchain is a public ledger, meaning that anyone in the world can view its contents; and
- Blockchain is immutable, meaning that information on the blockchain network cannot be deleted.

Inspection of court documents: The fact that the blockchain is public means that service via a NFT airdrop (including when linked to documents hosted on a public website) may be impractical in cases where the court documents contain witness evidence and confidential or private information, particularly in the case of an injunction. In theory, the world at large can find out about the proceedings once service is effected via the

blockchain.[8]

Tracking: Privacy legislation may also pose difficulties in using a tracking mechanism that can confirm the defendant received the service of process. It may be that the website hosting a hyperlink to court documents can deal with this by directing users to an appropriate privacy policy and/or cookies policy, but this would need to be considered on a case-by-case basis.

Deletion of data: The immutability of data on the blockchain makes it difficult (if not impossible) to delete the content of any NFT. The inability to delete data is generally contrary to many privacy laws, including the GDPR and the California Consumer Privacy Act ("CCPA"), due to data subjects having the right to request the deletion or rectification of their personal data. This means that it may be never be practicable to host court documents on the blockchain itself – parties will therefore need to rely on conventional internet sites to host information and/or documents (as was the case in *LCX*), with the blockchain token functioning more like a digital sign-post and not containing any personal data in its own right. The fact that the defendant may be anonymous and can only be identified by reference to a wallet address is irrelevant as privacy legislation defines personal information or personal data broadly. For instance, the CCPA[9] includes "unique personal identifier" as protected information, and the GDPR in the UK and EU also include an "identification number" or "online identifier" in their definition.[10]

Additionally, some laws grant a data subject has the right to request erasure of their personal data. If, several years after litigation were settled or concluded, a data subject whose identity corresponded with (or comprised) a wallet address wished to exercise their legal rights to have their personal data erased, this would not be possible if the information were hosted entirely on the blockchain.

Cybersecurity Considerations

Interacting with airdropped tokens: It is increasingly common for blockchain wallet owners to see malicious or spam tokens airdropped into their wallets[11], in what is essentially a Web 3.0 version of phishing. If malicious tokens are interacted with, they can do anything from directing wallet owners to fraudulent websites, to executing smart contracts that dissipate the entire contents of an owner's wallet. Parties in control of a wallet are therefore well advised never to interact with airdropped NFTs or click on hyperlinks from unfamiliar sources. With this in mind, the transmission of important legal documents via an airdropped NFT may well be ignored by the recipient.[12] This does not matter in practice, because the doctrine of service of court documents generally relies on constructive notice, much in the same way that serving documents by post or email work (i.e., it does not matter whether the party being served has actually seen the documents, so long as the serving party has taken the relevant step to effect service).

To the extent a law firm or claimant receives any follow-up token on the blockchain from the defendant (e.g. purporting to be a read-receipt or serving documents by way of return), they would equally be well advised not to interact with the token and seek the assistance of blockchain professionals.

Creating and sending the Service Token: Most legal advisors and claimants – particularly individuals – are unlikely to have the expertise to create an NFT without assistance from professionals experienced in blockchain and cryptoasset matters. It may therefore be necessary to work with trusted third party vendors to create a Service Token (together with a tracking mechanism if desired) and transmit it over the blockchain. It may also be

necessary to create a wallet from which to send the Service Token. To the extent law firms engage in activity of this nature, they will need to consider their internal IT and risk management policies, as many firms may have restrictions in place relating to cryptoassets. Firms may also wish to consider the implications of creating and/or sending a Service Token, with respect to any liability they could incur as a result of effecting cryptoasset transactions, particularly if the defendant somehow were to allege or suffer damage or loss after receiving or interacting with the token.

Conclusion

The prospect of serving court proceedings via NFT is an exciting development in litigation and may be appropriate (if not the only option) in certain types of litigation. However, parties and their legal advisors will need to think carefully and conduct a risk analysis before jumping onboard the NFT service bandwagon in any given case.

___

[1] *LCX Ag v. 1.274M U.S. Dollar Coin*, No. 154644/2022, 2022 WL 3585277 (N.Y. Sup. Ct. Aug. 21, 2022).

[2] [2022] EWHC 1723 (Ch).

[3] Seatlabs is an example of NFT-based event ticketing – https://www.seatlabnft.com/

[4] The Dubai Land Department, for instance, has leading the charge on adopting blockchain technology since 2017: https://dubailand.gov.ae/en/news-media/dubai-land-department-achieves-a-technical-milestone-with-the-adoption-of-blockchain-technology-in-cooperation-with-smart-dubai-and-other-partners/. HM Land Registry in England and Wales has been considering blockchain technology for a similar period of time.

[5] Goldfinch, a decentralised credit protocol, recently created Unique Identity (UID) NFTs. These are non-transferrable tokens representing KYC and investor verification on-chain: https://docs.goldfinch.finance/goldfinch/unique-identity-uid

[6] Exchanges should have KYC ("know your customer") records about all of their account holders, although it can take some time to obtain these details in practice – at the very least, a court order will likely be required and even then the accuracy of that data may be incorrect, especially in cases where the defendant is an alleged fraudster.

[7] https://www.hklaw.com/en/general-pages/lcx-ag-v-doe

[8] This directly conflicts with the procedure in England, for example, where court documents cannot be accessed by non-parties until all defendants have filed an acknowledgment of service, and even then witness evidence is generally not made available to non-parties.

[9] Cal. Civ. Code § 1798.140 (West).

[10] Article 4(1) of the GDPR (which also has effect in the UK by virtue of the DPA 2018).

[11] Ape-themed airdrop phishing scams are on the rise, experts warn

[12] The same may be said for service by email (i.e. a prudent email user would be well advised not to click on hyperlinks of an email they are not expecting to receive), which is consistent with the restrictive approach taken by the English Courts and civil procedure rules which only permit service by email where the recipient has expressly agreed to be served by such means.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber