# The Tulip Trading Timebomb

*The Quest For $4bn In Lost Bitcoin That Could Destroy Crypto*

by

Scott Robert Chamberlain

## 1. Introduction

1.1 The UK Court of Appeal's recent decision in ***Tulip Trading Limited v Van Der Laan & Ors*** [2023] EWCA Civ 83 is a first, dangerous step towards answering one of the major unresolved legal problems facing blockchain ecosystems: what is a blockchain and what legal rights and obligations exist between its various participants?

1.2 To participate in a blockchain, I download and run open-sourced code on a server synced with many other servers run by complete strangers around the globe to maintain a canonical, shared database that anyone with a valid key pair can use. But what legal relationships have I created? What is the nature of my relationship with the other server owners? With the users of that database? With the people who code the software I have chosen to run?

1.3 Well, thanks to Dr Craig Wright and his Tulip Trading Limited (Tulip) we may soon have some answers to some of these questions.

## 2. The Case Summary

2.1 This decision involved an appeal from a summary judgement that denied the UK was the right forum for the Tulip's dispute. In short:

(a) **Tulip Claims it Owns Bitcoin it Can't Access**: Tulip Trading Limited claims to be the owner of around $4 billion worth of bitcoin that it claims it cannot access because it claims it lost the private keys to the two addresses containing the coins, allegedly in a hack.

(b) **Tulip Claims Bitcoin Devs Must Grant it Access:** Tulip contends the floating team of developers who have code commit access to a one of the GitHub repositories for the open-source bitcoin code are Tulip's legal fiduciaries, and so have a fiduciary duty to write and deploy a software patch that sends the allegedly lost bitcoin to new addresses that Tulip does control.

(c) **The Defendants Claimed UK Should Not Hear Dispute & Trial Judge Agreed:** All defendants deny they have such a duty and, since all the defendants live outside the UK, the issue before the Court was whether the UK was the right forum for the dispute. The initial trial judge determined the UK was not the right forum because, while the dispute involved a UK plaintiff and UK property, there was no merit to the dispute and jurisdiction should therefore be refused.

(d) **The Court of Appeal Thinks UK Should Hear Dispute:** The Court of Appeal reversed this finding, holding that the claim was not without merit and should not summarily be denied on jurisdictional grounds.

2.2 This finding – that the dispute is not merely fanciful and should be heard - has alarmed many in the blockchain space, but it is unsurprising whilst potentially catastrophic.

## 3. Why the Decision is Unsurprising

3.1 The Court's ruling is unsurprising because:

(a) **The Issue Is Whether the Claim Is More Than Fanciful:** the issue before the Court was a technical one: without deciding the merits or relying on contested facts, is the Plaintiff raising a more than fanciful claim? Here, the Court adopted the principle that in dealing with jurisdictional issues, like other summary procedures, the Court should not decide "controversial points of law in a developing area on assumed or hypothetical facts." (per Briss LJ at paragraph 15).

(b) **The Claim is Clearly More Than Fanciful:** It is a low bar, and one Tulip cleared on appeal, probably correctly. The issue of whether coders owe duties to users is a real issue. Academic papers have been written on this very topic and the Court cites just such an article in its decision (*In Code(rs) we trust: Software Developers as Fiduciaries in Public Blockchains"* by Angela Walch of St Mary's University San Antonio Texas and UCL Centre for Blockchain Technologies and appears as a chapter in Regulating Blockchain, Techno-Social and Legal Challenges, edited by Hacker, Lianos, Dimitropoulos & Eich, OUP, 2019, cited by Briss LJ at paragraph 35).

3.2 The claim may not be strong and may not succeed, but the issue is real and not fanciful.

### Why The Claim Is "More Than Fanciful"

3.3 To pretend there is no issue is to ignore the special nature of blockchains and the revolution they allegedly inspire. One aspect of this revolution is the way mere data becomes a new form of property.

3.4 The legal issues arise as follows:

(a) **Data is Usually Information, Not Property:** Usually, information is not property as property rights usually subsist in either things I can possess (*choses in possession*) or rights I can assert (*choses in action*). If I have an excel spreadsheet that shows I owe you $100, that entry is just information. And if a delete it, nothing is lost: my debt to you remains. Nothing I do with my excel spreadsheet makes me either a custodian or a vandal of your property.

(b) **Blockchains Make Data a New Form of Property:** But in distributed systems, where a canonical shared state is maintained across multiple instances on independently owned servers such that the database can be used by anybody, is not owned/controlled by any single person, and persists unless a threshold number of servers are malicious or broken, that data entry ceases to be information and becomes a new form of property. Recent Court decisions in in New Zealand (***Ruscoe and Moore vs Cryptopia*** [2020] NZHC 728***)*** and UK (***AA v Persons Unknown*** [2019] EWCH (Comm) 3556) have confirmed bitcoin is a form of property. It is a special form of digital property that has independent existence outside the human mind, like a *chose in possession*, but exists only inside machines and code. As Briss LJ commented at para 72:

> *…The unusual factual feature of the present case is that literally all there is, is software. A physical coin has properties which exist outside the minds of people who use it and in that sense is tangible. Bitcoin is similar. It also has properties which exist outside the minds of individuals, but those properties only exist inside computers as a consequence of the bitcoin software. There is nothing else…*

(c) **Developers Help Make the Data a New Form of Property:** Once you accept that bitcoin is property created via software and existing only inside a network of machines, it is axiomatic that the code, and therefore the developers, have the potential to impact people's property. It is then only a short leap to wonder whether developers might owe duties to users to preserve the existence, integrity and worth of that property. Briss LJ picks up on this point at paragraph 15:

> *And crucially, asserts Tulip, it is the developers who control this software. On Tulip's case that control is very significant. In a bank the software developers as individuals will be tasked with maintaining the source code for the bank's accounts and payment systems, but they are subject to ultimate control by the board (and subject to regulation). The bank's developers have nothing like the control over the customer's assets which Tulip alleges the bitcoin developers have over bitcoin. These allegations are heavily contested by the developers in this case, who advance their case on decentralisation, but that cannot be resolved on this application or appeal.*

(d) **The Rules of This New Property Must Be Established:** So, if developers are involved in an activity that manifests a new form of property, the law will need to develop new principles concerning this new property. That inquiry will necessarily include whether and in what circumstances the developers owe duties to the people whose property relies upon the skill and diligence of the developers' code changes.

3.5 The answer might be that they owe no duties, but the issue is "live" and needs to be resolved.

## 4. Why the Decision is Alarming

4.1 The Court's decision means this case will proceed with no reason to believe it will be settled or abandoned prior to a binding decision. There are several reasons to fear this because:

(a) **Tulip Wins and Everyone Else Loses:** Tulip might win and that would be catastrophic; and

(b) **Tulip Loses but Nobody Else Wins:** Tulip might lose but for reasons that imperil chains other than bitcoin or ecosystem participants other than developers, principally miners/validators.

4.2 Let's unpack each of these in more detail.

## 5. Tulip Might Win and Everyone Else Loses

5.1 To long term crypto participants, the idea that open-source developers owe a fiduciary duty to help a user recover lost or stolen coins is absurd. Custody of the private keys is the responsibility of the user. But the idea of coders being liable as fiduciaries to people who use their code is the natural, default, knee-jerk position of both regulators and consumers.

### Why Tulip Might Win

5.2 Consider the following logic:

(a) **We Are Used to Redress:** We are used to a hub-and-spoke world where centralised institutions have responsibilities to their customers. Your money is not an independent asset: it is an obligation your bank owes you. Passwords are recoverable, stolen funds are refundable. There's almost always someone to blame and some form of redress.

(b) **Blockchains Lack of Redress Feels Unnatural:** It is only natural that regulators, confronted with the inflexibility of blockchain transactions, propose things like kill switches and transaction reversibility for smart contracts, private key recovery mechanisms, and software code audits. Given such a mindset, the idea that developers have a duty to users is not such a leap.

(c) **Crypto Concedes Coders Have Some Obligations:** In fact, it is an idea that even crypto enthusiasts concede when they acknowledge that it would be wrong for coders to insert hidden exploits into their code. Consider these four paragraphs from Briss LJ's decision:

> *75. A point which took on more significance on appeal than it may have had below is whether it is arguable that the developers owe at least some kind of fiduciary duty to bitcoin owners, different from the one pleaded by Tulip. The example would be a duty not to introduce a feature for their own advantage that compromised owners' security, referred to in judgment paragraph 74.*

> *76. I agree with the judge that it is indeed conceivable that relevant individuals – when they are acting in the role of developers – should be held to owe a duty in law to bitcoin owners not to compromise the owners' security in that way. It would be a duty which involves abnegation of the developer's self-interest. It arises from their role as developers and shows that the role involves acting on behalf of bitcoin owners to maintain the bitcoin software. It is also single minded in nature at least in the sense that it puts the interests of all the owners as a class, ahead of the developer's self-interest. It is, I would say, arguably a fiduciary duty. It is difficult to see what other sort of duty it could be.*
>
> *77. The significance of this conclusion is that it undermines part of the defendants' case, which if correct would deny any fiduciary duty of any sort. One of the points made in the judgment (at paragraph 73) is that there is no entrustment by owners because the developers are a fluctuating and unidentified body. Tulip does not agree with that characterisation. It is in fact part of the developers' case on decentralisation and, no doubt inadvertently, the judgment here accepted a highly contested fact as a premise. In my judgment, as Tulip submits on appeal ground 2C and 4A, this is a significant flaw in that part of the reasoning. Moreover, if such a point were sound, it would be just as good as a reason to deny the fiduciary duty I have just identified as arguable.*
>
> *78. A further step from here is to examine whether the arguable duties arising from the role the developers have undertaken include not only a negative duty not to exercise their power in their own self-interest but a positive one to introduce code to fix bugs in the code which are drawn to their attention. It would be a significant step to define a fiduciary duty in that way, but since the developers do have the practical ability to prevent anyone else from doing this, one can see why a concomitant duty to act in that way is properly arguable.*

(d) **Those Obligations Seem Fiduciary in Nature:** So, if coders have a (seemingly conceded) duty not to abuse their privileged position for their own self-interest, then that sounds like a fiduciary duty, which means they *are* fiduciaries.

(e) **So, They May Owe Other Duties:** Which means they may owe other duties of a fiduciary as well, perhaps extending to implementing code fixes for lost keys.

5.3 With this kind of logic, it is not fanciful that Tulip may win.

## Why Everyone Else Would Lose

5.4 A Tulip win would be catastrophic for crypto because giving users rights against other ecosystem participants is the best way to destroy crypto ecosystems. User rights (and therefore everyone else's obligations) inexorably lead to centralisation, in the process destroying the thing that is supposed to be unique and valuable about blockchain ecosystems.

5.5 In the case of obligations on coders, the first step would be coders incorporating to provide a liability shield, followed (probably very quickly) by professional indemnity insurance. That would in turn drive greater centralisation as insurers mandated risk management practices to control premiums and payouts. In time, the coders would become employees of a larger body that would soak up the insurance and management infrastructure costs and potential liability overhead, possibly even to the point of a licensed and regulated trustee (after all, it is a "custodian" of property).

5.6 Eventually, the whole chain would become controlled by a single entity responsible for issuing user credentials, and responding to complaints about scams, lost funds, and software bugs. Most chains already have foundations that would be the natural seed crystal for this entity. At that point there would be almost no benefit to having multiple canonical states preserved across multiple servers. May as well return to a single regulated entity controlling its own farm of servers that run code it maintains.

5.7 The irony is that at some point the level of centralisation must mean that there is no longer a valid argument that the information in the database is an independent form of property. Instead of having a counter-party free asset, I now have an IOU issued and tracked on a proprietary database owned and run by a single entity. My revolutionary crypto asset has become as generic as frequent flyer points or sky miles. So, treating coders as fiduciaries because they are custodians of someone else's property would ironically mean their independent property reverts to just being data recording an IOU.

5.8 At that point, the crypto movement dies.

## 6. Tulip Might Lose and Nobody Else Win

6.1 Many crypto enthusiasts might be comforted by the belief that, on a full trial and a thorough hearing of the facts, it is unlikely the Court would find coders owe any duties to Tulip. But it is not uncommon for judges to raise, but not dispose of, unrelated hypotheticals in reaching their decisions.

6.2 Even if Tulip loses, there's a risk judges inadvertently comment on other types of liability. This risk has two aspects:

(a) how the reasoning might apply to chains other than bitcoin, and

(b) how the reasoning might apply to participants other than coders, most notably miners.

### Impact on Chains Other Than Bitcoin

6.3 If Tulip loses it is highly likely the reasoning would be limited to the bitcoin chain. No other chain is quite so decentralised, especially in the way its code base has developed and been maintained.

6.4 Almost every serious chain other than bitcoin is managed by a foundation of some kind or a core development team. Even Ethereum, with its roadmap and scheduled releases named after capital cities, is infinitely more centralised than bitcoin in terms of the way the agreed canonical code is developed and deployed. So, even if bitcoin developers survive the Tulip claim, it is highly likely that comments made by the judges in reaching their conclusion will contain language that implies less decentralised developer teams do have fiduciary duties.

6.5 In essence, the case is likely to only fuel further cases as plaintiffs search for chains where the level of centralisation is somehow sufficient to enliven fiduciary duties. It is almost certainly the start of the inquiry into fiduciary duties on coders, not the final word.

### Impact on Participants Other Than Coders

6.6 One obvious, and legitimate, rebuttal to the claim that developers owe fiduciary duties to users is that they just write the code. It is the miners or validators that choose what code to run. It doesn't matter what the developers code if enough miners choose not to run it. Even if Tulip wins, its victory would be pyrrhic unless Tulip moves to bind the miners of the chain as well.

6.7 But this defence only shifts the debate from coders to… miners. Maybe *they* are the custodians because they own the machines on which the whole network runs. They choose the transactions, and they choose the code. And if the digital assets exist anywhere, they exist inside their machines. Further, they are the ones with an actual potential relationship with the users since they earn network transaction fees in exchange for including a user's transaction in their block. This makes it far more likely that miners or validators, rather than coders, collectively have duties to users related to the code they choose to run.

6.8 A proper, rigorous analysis of why coders do not owe duties to users could well result in a firm view that coders do not owe duties because those duties are owed by miners. Of course, there are plenty of legal and practical reasons why miners do not owe duties either. The point is that by shooting at, and missing, coders, Tulip may expose miners with the added wrinkle that miners are not party to the case and cannot defend themselves.

## 7. Next Steps

7.1 With the decision of the Court of Appeal, this case returns to the trial judge for hearing. It seems unlikely to settle given the diametrically opposed interests at play. The principal behind Tulip, Dr Craig Wright, not only has an obvious incentive to fight this $4 billion claim to the death but has a demonstrated appetite for legal proceedings. It should be watched closely, and the crypto industry should hope that the various coder defendants are well-resourced, well-represented and present a cohesive defence. It is a very important case.

Scott Robert Chamberlain

17 February 2023