(The following mini result came about as I was thinking about tools to tackle data availability. I'm sharing it here as it may be useful for other purposes.)

In cryptographic literature the topic of "fair exchange" is an active area of research that tries to solve the following problem. You have two parties, Alice and Bob. Alice has a piece of data D_A

(e.g. raw data identified by a hash, signatures, results of a database query, etc.) that Bob wants, and Bob has a piece of data D_B

that Alice wants. Can one design a trade mechanism that ensures atomicity, i.e. either both Alice gets D_B

and Bob gets D_A

, or neither Alice gets D_B

nor Bob gets D_A

?

A key result in the field is that, in the general case, fair exchange is impossible without a third party. This impossibility result can be problematic for decentralised applications. For example, Filecoin wants to atomically exchange files for payment, but they've resorted to the mitigation of slicing the files into many small chunks which are released tit-for-tat using a payment channel (see page 27 of the whitepaper). This is imperfect for example because the file may only be useful in its entirety, but the provider still gets paid for partially sharing the file.

As it turns out, fair exchange is possible without a trusted third party using cryptoeconomics (as opposed to pure cryptography). For that, Alice and Bob do the following:

1. They encrypt D_A

and D_B

using public keys Pub_A

and Pub_B

to produce E_A

and E_B

1. They swap (non-atomically) E_A

and E_B

(this shouldn't reveal information about D_A

or D_B

if padding is used)

1. They prove to each other in zero knowledge (e.g. using zkSNARKs or zkSTARKs) that E_A

and E_B

were correctly constructed

1. They post a large collateral (much larger than the value of D_A

or D_B

) into a fair exchange smart contract initialised with parameters Pub_A

and Pub_B

Once step 4 is completed, the smart contract starts a countdown during which Alice and Bob need to post the private counterparts of Pub_A

and Pub_B

to the contract otherwise the corresponding collateral is burned. At this point, Alice and Bob are both highly incentivised to release the private keys, thereby completing the fair exchange.