



Here's The One Thing You Absolutely Need In Crypto Smart Contracts

Users can face potential issues in security and transparency.

*By Erik Sherman
May 20, 2022*

One of the features of blockchain technology that cryptocurrencies rest upon is so-called smart contracts. These are programs built into transactions that can control or enforce the terms of a transaction.

In CRE applications like [property tokenization](#), smart contracts could automate payments of revenue shares, release funds for payment only after certain conditions like entitlement are met, or document allowable uses under a lease.

Tal Lifshitz, partner and co-chair of cryptocurrency of the digital asset and blockchain group at law firm Kozyak Tropin & Throckmorton, has seen them work in a broader context. "There are really, really smart people in the space, brilliant developers, smart contracts working perfectly and in such a way that leads me to believe that blockchain technology is inevitable to a certain extent," he tells GlobeSt.com.

And while that may be true, there are also potential dangers with smart contracts that CRE professionals thinking of using them need to address. The answer is often documentation and transparency.

A smart contract is computer code designed to run on some platform. But then, so is a copy of Word, a lease management system, or the software that runs the inbound logistics of Walmart.

As far as the user can see, it's a black box that does semi-magical things. There may be an instruction manual, but nothing that shows the step-by-step actions and decisions the software can take. An application itself offers nothing in that sense because, as executable code, a computer can read it, not a person. It is possible to reverse engineer code, but that is a complex process that doesn't guarantee to exactly reproduce what a programmer originally wrote. And even if it did, understanding existing code without documentation is a challenge for technical professionals let alone those who aren't.

To ensure agreement and mitigate risk that a smart contract might do something unexpected, prudence would suggest that there also be a detailed actual contract readable by humans, possibly with the source code.

Another reason for this is the need to protect against the possibility of human error. Ever use software only to find something didn't work the way it was supposed to? Most people who use computers of any sort have and all programs have bugs that must be found and removed and may only become obvious after use.

There is also the potential that someone intentionally writes a smart contract with nefarious intent so that it performs actions never agreed to by one of the parties. Done subtly, like skimming off small amounts over a large number of transactions that total significant sums, it could be a form of fraud that would be hard to detect and then, without source code and a human readable document that takes precedence and can be brought to court, if a situation came to that.