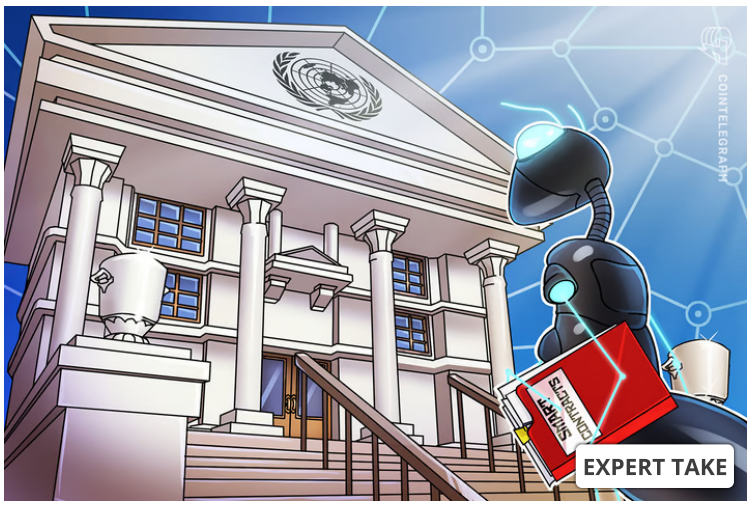
NICK SPANOS JUN 06, 2021

Hybrid smart contracts will replace the legal system

Hybrid smart contracts will change the world by revolutionizing the legal system that exists today.



The era of unintelligible contracts written in legalese by lawyers in $2,000 suits with degrees from Ivy League schools is over. The contracts of the next century will be hybrid smart contracts, written in code by programmers wearing $20 hoodies and living in their NYC-shared apartment.

What is a hybrid smart contract?

Smart contracts are self-enforcing contracts, written in code and executed by the blockchain. These smart contracts are great at sending and receiving money, and doing simple calculations, but they cannot access off-chain data, perform complex calculations or generate random numbers on their own.

Those limitations previously prohibited smart contracts from fulfilling many of the roles that traditional legal contracts currently hold. Now, the introduction of oracle networks onto the blockchain promises to solve this problem. Oracle networks can provide verifiable randomness, off-chain data

multiple validators so that no one validator has control over the oracle feed. Validators might also use different mechanisms to come up with the data they write to further increase robustness. For example, oracle networks that provide verifiable randomness might want each validator to use a different pseudorandom number generator.

Oracle networks are decentralized, so using an oracle network doesn't require sacrificing the benefits of decentralization that blockchain provides. A smart contract that makes use of an oracle network is called a hybrid smart contract.

Use cases for hybrid smart contracts

Once hybrid smart contracts have access to off-chain data through an oracle network, they can begin to replace traditional contracts. For example, weather insurance — a type of insurance that pays out in the event of extreme weather, is currently supported by traditional contracts. If an oracle network provides data on extreme weather events, weather insurance can be easily implemented by hybrid smart contracts instead. In general, any contract that pays out based on real-world events can be implemented on the blockchain, as long as there is an oracle network that can provide that off-chain data.

Hybrid contracts can also implement mechanisms that have higher computational complexity than their non-hybrid counterparts. For example, the Vickrey-Clarke-Groves (VCG) algorithm is a sealed, bid auction mechanism. Google and Facebook use VCG to run their ad auctions. The only problem with VCG is that it's difficult to compute. It would be prohibitively expensive to implement a VCG mechanism entirely on the blockchain. But, if the computation was delegated to off-chain computing using a hybrid smart contract, VCG could be cost-effective and implemented on the blockchain.

Oracle networks that act as random number generators can, of course, support multiple on-chain gaming and gambling matches, but they also can support randomized algorithms and mechanisms, some of which are more efficient than their non-random counterparts. One example is an auction mechanism called a candlestick auction, which is equivalent to the standard English auction except that instead of ending after a fixed period of time, the auction ends at a random time. EBay users may be familiar with the scalping problem in which nearly all bidding activity takes place just before the auction ends.

This can be frustrating for buyers, as they have little information about the actual price the auction will clear at before the auction ends. The candlestick auction solves that problem by incentivizing bidders to place bids early so that they can get them in before the auction ends. Without a random number generator, it would be impossible to implement a candlestick auction or any other randomized mechanism or algorithm on the blockchain.

The advantages of hybrid smart contracts over traditional contracts

Unlike traditional contracts, smart contracts are enforced by the blockchain, meaning that there is no need for an external court system to enforce the contracts. Without a costly court system, contracts are cheaper, so more peer-to-peer transactions can be governed by contracts rather than trust.

Contracts between firms located in different countries are often challenging, since navigating the different court systems is expensive, and usually, the judicial systems of one nation have limited power over corporations from other nations. Hybrid smart contracts do not share this weakness; they don’t see nationality at all.

Enforcing traditional contracts through the courts is not only expensive but also introduces uncertainty into the outcome. There will always be a chance that lawyers uncover some arcane loophole buried in the basement of a haunted house that completely voids the contract. Even when the contract is airtight, the contracting parties rely on their government’s continued goodwill to ensure that the contract is enforced.

The recent moratorium on evictions in many states within the U.S. and countries around the world is an example of this. Landlords and tenants signed an agreement under the guise

that if rent was not paid, the landlord would have legal recourse against the tenant in the form of eviction. I am not going to argue about whether this decision was justified; that's a discussion for policymakers. What is not up for discussion is that this action taken by governments around the globe effectively voided every single rental agreement that was in place at the time.

This change didn't only affect the tenants who were unable to pay their rent, it also effectively voided rental agreements between landlords and tenants who could pay. Even tenants who could pay their rent would not be subject to eviction, which meant that some of those tenants chose not to pay either. Whatever your opinion on the eviction moratorium, it is clear that contracts that can be burned at any time by a government official with a rubber stamp are not desirable when compared with hybrid smart contracts.

In the coming years, traditional legal contracts will be replaced by hybrid smart contracts, as they are faster, more efficient and less vulnerable to legal loopholes. They are less expensive and can reach across borders just as easily as within borders.

The views, thoughts and opinions expressed here are the author's alone and do not necessarily reflect or represent the views and opinions of Cointelegraph.

Nick Spanos is a co-founder of the Zap Protocol, the decentralized oracle solution for smart contracts. An early pioneer, Nick founded Bitcoin Center NYC in 2013, the world's first-ever physical crypto trading floor, located across from the NYSE.

#Blockchain #Law #Government #Smart Contracts #Decentralization #Technology

Add reaction