Twitter Thread by Emin Gün Sirer



Emin Gün Sirer
@el33th4xor



Back with another #FreeLoveFriday. Last time, we covered how Mastercoin/@Omni_Layer pioneered digital asset issuance on blockchains. Today, let's discuss @Chainlink and the vital role it plays in connecting blockchains to the real world.

> Back with another #FreeLoveFriday. My first thread focused on what I love about Bitcoin, and features we borrowed for @AvalancheAVAX. Today, let's focus on @Omni_Layer, or as OGs knew it, Mastercoin https://t.co/fXFgmaeUEz
>
> — Emin G\xfcn Sirer (@el33th4xor) January 15, 2021

I have said repeatedly that digital asset issuance is the killer application for blockchains. The next frontier is bringing real world assets to networks like @AvalancheAVAX, but we often face a significant problem:

Namely, how do you get data from the real world onto blockchains and into applications running on them? More critically, how do you achieve that securely and transparently in real-time? Smart contracts are tamper-proof, but they're only as reliable as their input data.

Enter ChainLink in September 2017, with a whitepaper outlining a vision for a decentralized network of “oracles,” entities that inject facts from the external world into blockchains in a suitable format for smart contracts.

Until ChainLink, oracles were trusted and centralized. This is a huge problem for high-value assets and smart contracts. High value projects, such as @CelsiusNetwork, @synthetix_io, @Aaveaave and others depend critically on oracle data.

As these networks grow to handle more value, “Oracle Extractable Value” goes up and oracle security becomes a significant issue.

In 2018, ChainLink commercialized “Town Crier” technology built by @initc3org at Cornell. Town Crier uses Intel’s SGX technology to harden their defenses against tampering and reduce the trust required of the oracle operator.

@SergeyNazarov and team have done an amazing job in overhauling what we knew about oracles, strengthening smart contracts, and spurring healthy competition with more oracle projects.

So what’s next? I think one of the biggest challenges facing oracles is how to deliver granular, real-time data at low cost. I have some ideas for how to solve these for good, but I’ll save them for another thread.

Let’s just say that Avalanche subnets and ChainLink’s decentralized architecture are a very good match, and that’s one of the many reasons why we have forged a partnership.