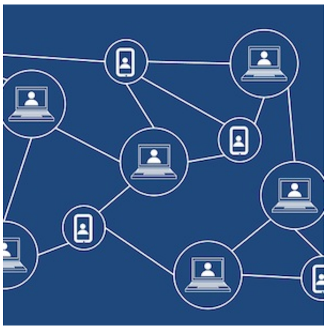
HealthManagement
Promoting Management and Leadership

A real use for smart contracts?



Blockchain technology has given rise to new concepts such as "smart contracts", which have the potential to be a game changer especially when it comes to facilitating business transaction processes. For example, if your flight is cancelled but you purchased flight insurance, a smart contract might instantaneously pay you after getting an update from a trusted source of flight times.

Smart contracts are computer programs that are stored in a blockchain, or digital ledger. Such contracts can generally be used to automate the transfer of crypto-tokens between users, according to agreed-upon conditions. However, before smart contracts can be of use in everyday transactions, they need a reliable way to connect with events in the real world.

The good news is that a tech startup, Chainlink, has tackled the so-called "oracle problem" that has kept smart contracts from responding to actual events. “Oracles” are real-time data feeds that deliver a variety of things like weather data, currency exchange rates, airline flight information, and sports statistics to smart contracts.

Chainlink is combining its software with a trusted hardware system called Town Crier, developed by a leading academic cryptocurrency research group, in the hope of finding solutions to the problem. Chainlink’s CEO, Sergey Nazarov, explains that the oracle services introduced to date defeat the purpose of using a blockchain in the first place. In Ethereum, for example, all the participating nodes in the network compute every smart contract, making the programmes virtually impossible to shut down.

Nazarov points out that today’s oracle services are too centralised, such that they represent "single points of failure" that make targets for tampering. The collaboration between Chainlink and Town Crier means the two systems can allow blockchain-based services to interact with real-world events with a greater degree of trust than is possible from today’s oracle services. Town Crier, a product of Cornell’s Initiative for Cryptocurrencies and Contracts, works as a “high-trust bridge” between the Ethereum blockchain and HTTPS-enabled online data sources.

The core component is a programme that runs inside an isolated piece of hardware called a secure enclave. The enclave’s function is to protect the program from malicious attacks and keep the computation confidential. It receives queries for data from smart contracts — for example, a flight insurance contract may query whether a flight was cancelled — and then it retrieves answers from websites and relays them back to the blockchain.

Using cryptography, and assuming trust in the hardware, it provides proof to the flight insurance contract that the data really came from Town Crier and hasn’t been messed with. Town Crier may be more trustworthy than other data feeds, but on its own it doesn’t offer the reliability that decentralised systems do.

That’s where Chainlink comes in. Its software orchestrates decentralised networks of oracles to draw on multiple sources of data for smart-contract-based services so that they don’t have to rely on a single one. As such, the Chainlink service provides proof on the blockchain that the data is in fact the information it committed to delivering. The combination of Chainlink’s software with the Town Crier hardware system, according to Nazarov, is the first “provably secure, decentralised oracle network.” Customers can pay for different levels of decentralisation, and the nodes can make money in return for submitting data, Nazarov adds.

Source: MIT Technology Review
Image source: Pixabay

Published on : Mon, 26 Nov 2018