

WHAT ARE SMART CONTRACTS IN BLOCKCHAIN?

Smart contracts, also called distributed apps, are very popular nowadays. The term “smart contract” was first used by Nick Szabo in 1997, long before Bitcoin was created. He wanted to use a distributed ledger to store contracts hence the origin of smart contracts. Smart contracts are just like contracts in the real world the only difference being that they are completely digital. A smart contract is a tiny computer program that is stored inside a blockchain.

As a Crowdfunding Platform

Smart contracts utilize the same concept as Kickstarter, the large fundraising platform. Product teams can go to Kickstarter, create a project, set a funding goal, and start collecting money from others who believe in the idea. Kickstarter is essentially a third party that sits between product teams and supporters. This means that both of them need to trust Kickstarter to handle their money correctly. If the project gets successfully funded, the project team expects Kickstarter to give them the money. Supporters want their money to go to the project if it was funded or to get a refund when it hasn't reached its goals.

But with smart contracts we can build a similar system that doesn't require a third-party like Kickstarter. We can program the smart contract so that it holds all the received funds until a certain goal is reached. The supporters of a project can now transfer their money to the smart contract. If the project gets fully funded, the contract automatically passes the money to the creator of the project and if the project fails to meet the goal, the money automatically goes back to the supporters.

Since smart contracts are stored on a blockchain, everything is completely distributed. With this technique, no one is in control of the money. Smart contracts are trusted in such operations because information is stored in a blockchain and are immutable and distributed. Being immutable means that once a smart contract is created, it can never be changed; no one can tamper with the code of your contract. And being distributed means that the output of your contract is validated by everyone on the network. Therefore, a single person cannot force the contract to release the funds because other people on the network will spot this attempt and mark it as invalid. Tampering with smart contracts becomes almost impossible.

Smart contracts can be applied to many different things, not just on crowdfunding. Banks could use it to issue loans or to offer automatic payments, Insurance companies could use it