What Is a Smart Contract?

By

Werner Vermaak

Published on:
November 26, 2020

Smart contracts are already a pretty important part of the crypto space, especially as DeFi has taken off — so what are they actually used for?

Table of Contents

A **smart contract** is an open-source **blockchain** protocol that embeds the voluntary terms of an agreement between a buyer and a seller as a set of predefined rules in computer code and self-executes them when they're met. For example, a smart contract could self-execute when a price or funding limit is reached or a certain period of time has elapsed. A smart contract enables credible **transactions** to be conducted without the need for intermediaries, allowing businesses to interact with enhanced legal stability and efficiency.

Smart contracts enable business parties to manage, access and govern asset tokens for any type of business object on a transparent and immutable digital

ledger that is distributed to all parties and requires consensus for updates. A smart contract is not “smart” in the true sense of the word, it is rather only as clever as its creators.

Importantly, if done right, smart contracts offer additional benefits over traditional legal contractual mechanisms, such as enhanced security, real-time monitoring and compliance and less auditing. All these advantages add up to significantly lower the cost and increase the speed of transacting between businesses, as parties can reach an agreement, formalize it in a contract and enforce this much sooner and more cost-effectively than before.

Furthermore, smart contracts can reduce organizational bureaucracy and offer greater transparency over traditional contracts by establishing a decentralized autonomous organization, or **DAO**, which governs the smart contract independently.

Much like traditional contracts, smart contracts can be applied to a vast array of purposes in industries like telecoms, banking, finance, insurance, education, media and more, such as to create financial derivatives, legally define ownership, set up rental agreements, manage intellectual property rights, establish usage agreements or run crowdfunding projects.

A smart contract could, for example, ensure that a new vehicle is delivered to a buyer by a deadline or that funds are released on pre-agreed terms.

The Origin of Smart Contracts

The concept of smart contracts was first introduced in 1994 by the pioneering cryptographer (and viable **Satoshi Nakamoto** candidate) Nick Szabo, who

created the pseudo-cryptocurrency Bitgold in 1998. Szabo defined it as a computerized transaction log that executes the terms of a contract.

However, it wasn't until the advent of the Ethereum network two decades later that smart contracts began to catch on and deliver on their promise. Unlike **Bitcoin**, Ethereum is more than just a digital store of value, and the virtual platform has served as a home for tens of thousands of new projects, first during the 2017 ICO boom and now for the new 2020 wave of **decentralized finance (DeFi)** applications that run on the Ethereum network as **ERC20** tokens and smart contracts.

How Smart Contracts Work

Smart contracts can work on their own, interact with other smart contracts and even connect to external data sources through the use of **oracles** like **Chainlink** (LINK) and **Band Protocol** (BAND). For example, a series of smart contracts can be set up to create full network autonomy, where each contract will automatically execute only if the previous one has concluded.

There are several main parts, or objects, to a smart contract. These are 1) the signatories (two or more contract users), 2) the agreement subject which exists within the contracts environment, such as a crypto asset, and 3) specific terms, written in the relevant native programming language, that define the protocol's rules and rewards or punishes users based on their behavior.

Smart Contracts and Security

Smart contracts may use a combination of trusted security and encryption tools like HTTPS and SSL certificates, and are also usually subjected to third-party audits to ensure their safety. The rapid ascent of the DeFi space this year has created a slew of new protocols largely untested, rushed to a live environment and not properly audited, if at all. As a result in 2020, hundreds of millions of dollars have been lost by investors due to hacks, exit scams and software bugs.

Since September 2020 alone, the DeFi protocols **Value**, **Origin**, **Akropolis** and **Harvest** have suffered smart contract breaches. It is advised to tread careful when interacting with a DeFi smart contract and do your own research on the project.

In general though, the future of smart contracts are very bright, with a number of growing virtual asset networks like **NEO**, **Ontology** (ONT), **Binance Chain** (BNB) and **Cardano** (ADA) competing with **Ethereum** and further evolving their use.