GEORGETOWN UNIVERSITY
Psaros Center for Financial Markets and Policy
McDONOUGH SCHOOL of BUSINESS

Decrypting Crypto: Smart Contracts

Edited by Yaya J. Fanusie, Visiting Fellow
Written by Julen Payne and Stella Millspaugh, Research Assistants

Key Insight

Smart contracts enable expansive programmability within blockchains, offering complex digital transactions and applications in decentralized platforms. There is significant work in the crypto space to improve and accelerate the use of blockchain smart contract usage, but regulatory and legal issues need to be sorted out for wider adoption.

Summary

Smart contracts are self-executing digital contracts, or agreements, on a blockchain that are automatically executed when certain conditions are met. In principle, they are the same as traditional contracts, except the terms are established and executed as code on a blockchain that cannot be altered after deployment. A key feature of smart contracts is their programmability, which allows contract creators to define complex requests and behaviors directly within the contract code. They are typically used for decentralized applications available to any blockchain user who fulfills the requirement for executing the contract. The purpose is to remove the need for a trusted third party or intermediary to enforce the terms of the contract between actors.

Key Facts & Considerations

- Blockchain smart contracts are not legally binding unless explicitly linked to a legal agreement operating in the real world. There is significant legal and policy work needed, likely including major legislation, in order to enforce blockchain smart contracts within the legal system.
- All smart contracts deployed on a permissionless blockchain can be viewed publicly by users to ensure their legitimacy, and they are not editable after being deployed.
- While any smart contract can be launched on a permissionless blockchain, users should be careful to ensure that all smart contracts they interact with are professionally audited by reputable third parties to ensure legitimacy, cybersecurity, and freedom from bugs. Although legitimate, high-quality blockchain projects conduct code audits as a best practice, there currently are no agreed-upon code auditing standards for smart contract development.

Key Institutions

- Chains: Ethereum, Solana, Binance Smart Chain, TRON, Arbitrum
- Research: Ethereum Foundation, Consensys, MIT Digital Currency Initiative, Chainlink Labs
- Companies: Chainlink, Uniswap, Aave, MakerDAO
- Auditors: Trail of Bits, OpenZeppelin, Zellic, Consensys

Background

Smart contracts were introduced as a concept by the mathematician Nick Szabo in 1994. However, the Ethereum blockchain was the first software protocol to offer a simple yet dynamic way of creating digital contracts. The simplest and most apparent usage of smart contracts was for financial transactions, allowing two parties to exchange monetary value online without a central authority to oversee transactions. While Bitcoin was the first blockchain software protocol, its coding does not support complex digital contracts. Ethereum allowed a wider range of smart contracts to be developed and deployed on the blockchain itself, including smart contracts that create new tokens.

Key Benefits

- Instantaneous peer-to-peer execution without traditional settlement delays
- Collateralized, real-time lending without intermediaries
- Token creation and programmable issuance for various use cases
- Seamless transfer of asset ownership across blockchain networks
- Digital assets securely locked in neutral custody

Policy and Regulation Issues

Legal frameworks around smart contracts have yet to develop in full and the technology faces challenges around regulation and enforcement. Smart contracts on blockchains may not necessarily be recognized by the real-world court system, and recent government actions have raised complex legal questions that are still being litigated. For example, in recent years the United States Department of Justice has announced criminal cases that have sought to put certain non-custodial smart contract protocols under the definition of a money-transmitting business under Section 1960 of the Bank Secrecy Act (BSA). While money transmitters are generally defined as entities that transfer funds on behalf of the public or facilitate transactions in exchange for a fee, many smart contracts operate without custody of user funds or centralized control. This raises questions about how such protocols align with existing regulatory definitions and where legal responsibility should be assigned in decentralized systems. Some legal issues are being clarified, however. A U.S. federal court ruled in early 2025 that immutable smart contracts on blockchains can not be considered property because they technically can not be controlled or owned by anyone.

Example Use Case

Aave is a decentralized cryptocurrency lending platform that allows people to take out loans from pooled crypto that others have invested for liquidity purposes. Users who lend their money to Aave earn interest on their deposits. Smart contracts in the platform guide each step of the activity. When taking out a loan, borrowers have to submit some form of collateral in the case that they cannot pay back their loan. If the value of the collateral falls below a certain threshold set by the smart contract, the collateral is automatically liquidated to repay the loan.

Image Courtesy of Szakiel, Patrick. How Smart Contracts Are Changing the Way We Do Business. 2022. G2, https://www.g2.com/articles/smart-contracts.

For more information, please visit our website finpolicy.georgetown.edu or email cfmp@georgetown.edu