

Making and enforcing agreements speedily, smoothly and securely is essential to all kinds of financial and business transactions. Traditional legal contracts depend on intermediaries, including lawyers to draft legally sound documents, and the justice system to enforce penalties in the case of wrong doing.

Leaders and institutions are looking to smart contracts as a way to streamline and automate some of these steps. Can smart contracts combine the speed and convenience of the digital with the security of traditional enforcement methods?

What is a smart contract?

Smart contracts, also known as blockchain contracts, self-executing contracts, or digital contracts are not contracts in the legal sense. More accurately, they are tiny computer programs stored on a blockchain-based platform which execute all or part of a contract or agreement if certain conditions are met, without the need for a middleman. For example, a smart contract could say that if one of the contract parties completes an action, funds are released from the other party.

A vending machine is a good real-world example of a digital contract. The customer inputs money and selects an item. The vending machine program checks if the amount of money is correct, and if so, releases the item. The vending machine program then checks if the customer needs change, and releases the change according to which coins are available. All of this simple logic is easy to program and can be carried out automatically without human decision-making.

Benefits of blockchain smart contracts

Smart contracts based on a blockchain have additional benefits compared to a simple vending machine. The protocol behind the technology allows multiple parties to maintain consensus on the terms and changes made to a shared agreement, without needing to know or trust one another.

A smart contract can be self-contained, or call or refer to other smart contracts, or even draw on external sources of data such as the price of a stock on the S&P500.

No middleman

Cryptocurrency blockchains are capable of receiving, storing, and sending funds. Funds can be released when conditions are met, and financial penalties for breaking a smart contract can not only be defined within the smart contract, but implemented automatically.

This removes the need for a trustworthy middleman to hold funds, verify the payout conditions, judge whether the contract has been breached, or enforce financial penalties and recover funds. Cutting out an intermediary can result in significant cost savings.

Tamperproof

The smart contract is stored on a distributed ledger, where each node of the blockchain network has its own copy – the contract cannot be changed or tampered with after its creation without the agreement of a majority of nodes on the blockchain. Transactions on the blockchain can be instantly verified, and digital signatures validate ownership of the fund involved.

Fast, convenient, accurate

Smart contracts can be verified and executed much faster than traditional contracts – near instantaneously when conditions are met. This would take much longer, and be open to human error, if carried out manually. Processes and information spread across multiple ERP systems and databases can be referred to by the smart contract, further streamlining execution.

Limitations of blockchain smart contracts

Vulnerability to hacking

As smart contract code executes automatically, bad actors will naturally be drawn to find exploitable loopholes – there [multiple examples](#) of hackers making off tens of millions of dollars worth of cryptocurrency. Instead of trusting and paying for a legal intermediary, signatories to a smart contract now have to trust and pay whoever writes the smart contract code. Researchers estimate that [45% of smart contracts](#) in Solidity, Ethereum's programming language, are vulnerable to attack.

Unusual or subjective cases

Computer programs are great at automating processes where the input and output are clear – such as our vending machine example. This is still true when the calculations involved are very complex. However, computer programs are not optimal for dealing with unusual or subjective cases. They are also vulnerable to actions in 'bad faith'. Dealing with such cases would involve using a human intermediary anyway, or ensuring the smart contract code is programmed with all unusual cases in mind.

Not for real assets

Enthusiasts claim that blockchain-based smart contracts could be used for property letting, vehicle renting, and more. However, use cases that effectively link real assets to smart contracts are very theoretical. For now, smart contracts are only effective in the digital domain.

Which blockchains support smart contracts?

Smart contracts run on a blockchain, but not all blockchains support smart contracts. The largest and best known blockchain, BitCoin, does not support digital contracts. Most smart contracts today are coded onto the Ethereum blockchain. Cardano, EOS and Tron are other cryptocurrency blockchains which smart contracts.

Smart contract applications

Blockchain-based smart contracts are already being tested and used by some industries. It's important to note that in nearly all cases so far, the blockchains have not been public. Businesses using smart contracts typically use private blockchains that connect and are maintained by a small number of parties.

Securities trade clearing and settlement

Settlement and trade clearing typically includes multiple levels of approval, internal, and external reconciliations of varying levels of complexity. Discrepancies between calculations and IT networks of the counterparties can lead to lengthy settlement delays and resolution processes.

Working from the same ledger – a single source of truth – and automatic execution of clearing calculations and approval workflows offers an immense opportunity to streamline this process. Santander Innoventures estimated in 2015 that “Blockchain could reduce banks’ infrastructure costs attributable to cross-border payments, securities trading and regulatory compliance between \$US 15–20 billion per annum by 2022.”

Supply chain document handling

Global supply chains, even in the 21st century, are deeply reliant on paper-based systems. Banks and trading parties physically transfer documents like letters of credit and bills of lading to one another so they can be signed by multiple parties. While this system is open to fraud, speedy digital documents are too easy to forge.

A blockchain-based distributed ledger could eliminate some of these issues by providing all parties with secure digital versions of documents, verified digital signatures and smart contracts to automatically release payments when the appropriate signatures are collected. [At least 7 major banks, including Barclays](#), and a major insurer are working on proof-of-concept in this space.

In conclusion, blockchain-based smart contracts can have powerful advantages over existing solutions. This is most true for use cases where repetitive manual tasks are performed by counterparties and where the same network of parties perform transactions between each other. Transacting activities such as approvals and calculations, which both have clear yes and no criteria, and are prone to lag and error, stand to see the most benefit.

Nevertheless, the technology is not without limitations and still hasn't been tested at scale. The code itself as well as code auditing becomes a new source of distrust, as can any data pulled in from external sources.