Smart contracts summary

Smart contracts are user defined programs that specify rules governing transactions, brining new challenges as this is implemented on new blockchains. Bitcoin is neither expressive or user-friendly, the programming language is uses for scripts is not Turing-complete, so writing arbitrary programs on the bitcoin blockchain is near impossible.

However, some new chains, such as Ethereum, do provide this feature. To limit computation (so that miners can do their job), Ethereum uses a system with “gas” to make users pay for the computation. Another problem with smart contracts is that some things are near impossible to do. Contracts should be deterministic, so that the same state is replicated on every machine that runs them, but this is hard to do when they require input from outside, sometimes called “oracles”. If something is retrieved from outside the chain, this will have to be retrieved by every node on the network. Standard blockchain systems also often lack not only performance to run arbitrary applications but also confidentiality. One new proposal to solve this is called Ekiden, which uses trusted execution environment, separating consensus from execution, which in turn greatly increases performance and throughput.

Obviously, a big advantage of smart contracts over standard contracts is that these contracts can run decentralized on blockchains, as well as being completely transparent. It is easy for both/all parties to verify the code and make sure that the contract does exactly what it is supposed to do, as it is public on the blockchain.

Smart contracts are also, as all transactions, immutable. This might present some difficulties when things need to get changed.