Smart Contracts

A smart contract automatically enforces a contract between two parties, with a credible digital ledger, all without the need for third parties. A smart contract is a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract. Code is injected into the blockchain, and it is automatically enforced without any need for user intervention or third-party verification. Smart contracts are frequently considered a cryptocurrency's "killer app" because they have the potential to replace traditional contracts. Smart contracts have enormous upside potential to be a disruptive industry affecting anyone involved in ledger verification, contracts, or sales.

The improved ease of transaction verification resulting from smart contracts will lower service fees worldwide. Banks are already internally using it to improve the efficiency of processing and clearing payments through automation. More complex smart contract examples include real-time auditing and risk assessments by credit companies, merchant processors, and accountants.

Various protocols can do smart contracts, the larger ones are Ethereum and EOS with others like Cardano, Steller, Tron, etc looking to gain their space. Ethereum smart contracts are robust, versatile, and powerful thanks to the complex coding capabilities available using Solidity.

It is premature to say that blockchain smart contracts will eliminate lawyers. The fatal flaw is the idea of committing code to the blockchain itself — it is permanent, costly (in ETH), and the blockchain must judge every single transaction of the smart contract, even if there are tons of transactions. What makes contracts so powerful is that a judge is not necessary for a transaction, but only as a backup in the event of a breach. Other 'smart contract platforms' such as Ethereum and Tron completely miss this fundamental insight of contracts.

A solution is a tool that was first created to make microtransactions instantaneous and affordable in Bitcoin: the Lightning Network. The design of the lightning network fully grasps this contracts concept. With lightning, millions of transactions can take place between two individuals without needing the judge at all. The judge is the blockchain. And the judge doesn't need to enforce every transaction, just those that may be in breach of contract. Using a lightweight tool like the Lightning Network instead of the sledgehammer of the entire blockchain makes sense. Imagine if every computer had to store every e-mail, to receive any. That's how blockchains work. Lightning Network allows computers to make blockchain transactions, only storing the data they care about — their own money. A smart contract system built on top of Bitcoin allows the judge (the blockchain ledger) to be invoked only when needed, not every time.

Simplicity is crucial for smart contracts by forming the basis of predictable execution. In this light, Bitcoin's simplicity and security shines through. The key factors for smart contracts are trust, reliability, and convenience — and Bitcoin's massive gravity means Bitcoin smart contracts are inevitable. Current solutions for Bitcoin smart contracts include side-chain RSK (Rootstock) as well as the Lightning Network.