BLOCKCHAIN STUDENT ASSOCIATION for Syz

What is a smart contract?

Exploring Smart Contracts: A Technical and Financial Perspective

The innovation of smart contracts is one of the most significant advances in the blockchain space, particularly with the development of Ethereum, which marked a pivotal moment in broadening the applications of blockchain technology beyond Bitcoin's initial scope.

Ethereum's creation was driven by the limitations of Bitcoin's scripting capabilities, which restricted the execution of complex agreements. Vitalik Buterin's vision, outlined in the Ethereum white paper in 2013, proposed a platform that could facilitate more sophisticated applications through smart contracts and secondary tokens. This concept was revolutionary, as it extended blockchain utility beyond simple transactions to a broader range of decentralized applications (dApps), funded and developed through an innovative approach that leveraged the potential of blockchain technology for more than just cryptocurrencies.

Smart Contract Fundamentals

In short, a smart contract is a piece of code posted on the blockchain and accessible by those who have permissions, which are assigned when writing the code. They are automatically executed when a specified input is provided. These digital contracts mimic the logic of physical contractual clauses, ensuring that all parties to the contract can trust the outcome without the need for intermediaries. The idea can be paralleled with traditional automatic systems, like vending machines, where specific inputs yield predetermined outputs without human intervention.

Smart contracts on the blockchain stand out for their censorship resistance and immutability. They are securely stored across a decentralized network, preventing any single entity or a single state from stopping or altering their execution. The immutability and permanent storage is due to the "read-only" blockchain storage, in contrast to the "read and write" capability of traditional databases. Additionally, smart contracts are protected and validated through a blockchain consensus, enhancing their security and reliability far beyond conventional centralized systems.

Operation and applications of smart contracts on Ethereum

On Ethereum, smart contracts are written in Solidity (the name of the programming language) and are compiled into bytecode, which the Ethereum Virtual Machine (EVM) can interpret and execute. The EVM is a software that processes the smart contracts on Ethereum. The deployment of a smart contract to the Ethereum blockchain involves sending a transaction on the network containing this bytecode. Once deployed, the contract has an address through which users can interact with it, either to query its state or to execute its functions, provided the transaction meets the necessary criteria defined in the contract. It is important to note that while a smart contract doesn't need any

supervision to be executed, it is not self-executable, as some external input needs to trigger it.

The decentralization of applications (dApps) has been a significant area of growth, with smart contracts at its core. These applications span various sectors, including finance, where they've given rise to decentralized finance (DeFi) platforms. DeFi uses smart contracts to recreate traditional financial services like lending, borrowing, and trading without central financial intermediaries, leading to protocols that offer automated, transparent, and more accessible financial services. Most of these applications are called permissionless, meaning that anyone, from any country and with any financial background can access them. This is in stark contrast with the actual banking system in which you need a certain score to obtain certain benefits.

A notable application of smart contracts is the creation of tokens, particularly fungible (ERC-20) and non-fungible (ERC-721 and ERC-1155) tokens. These tokens can represent anything from currencies to unique digital items and are essential for the operation of decentralized exchanges (DEXs) and automatic market makers (AMM). These platforms allow for the trustless exchange of assets by using liquidity pools rather than traditional market-making mechanisms, a concept that has fundamentally changed how asset exchanges operate.

Advantages and Limitations

Smart contracts bring automation, reducing the need for trusted intermediaries and thereby potentially lowering costs. Their transparency,immutability and permissionless attributes build trust among parties. Furthermore, the concept of 'composability' in DeFi, where smart contracts interact and build upon each other, extend the potential and horizons of this technology.

However, the innovation comes with challenges, particularly around the cost of transactions (gas fees) and the complexity of interfacing with the real world. Another important problem that needs to be addressed is how to fetch external data onto the blockchain. Indeed, as the blockchain is a network by itself, data that is not inherent to the blockchain needs to be put onto it. Furthermore, we need to ensure that this external data is correct, as once it is on the blockchain, it is there forever. This is where Oracles such as Chainlink come into play. They serve as bridges between blockchain and external data, but they introduce a layer of trust and potential vulnerability. Furthermore, the immutable nature of smart contracts means that bugs or vulnerabilities can have serious, irreversible consequences, as seen with multiple protocol hacks. This is why it is important for the various projects and protocols to carry out security audits of smart-contracts, and for investors, to check whether these have indeed undergone a security audit.

Conclusion

Smart contracts are a cornerstone of the blockchain revolution, offering a framework for automating complex agreements and enabling a plethora of applications that extend far beyond simple cryptocurrency transactions. As the technology matures and the community continues to innovate, the potential applications of smart contracts are vast, promising to transform not only the financial industry but numerous other sectors as well. However, realizing this potential will require ongoing attention to the challenges of security, scalability, and integration with the broader digital and physical world. Finally, the realm of smart contracts does not only stop at the Ethereum blockchain. Beyond Ethereum, the universe of smart contracts is vast and diverse, with numerous blockchains developing their unique languages and ecosystems. Each offers distinct features, optimizing for factors like efficiency, security, and developer friendliness. As we navigate these waters, the future of smart contracts promises not just technological transformation but a foundational shift in how we conceive of and execute agreements in the digital age.