Kasper Borgbjerg
kasperib@uio.no

Smart contracts

The concept of smart contracts has caught a massive updraft with the emergence of Ethereum, NFT's and DAOs (decentralized autonomous organizations), but what are these mysterious smart contracts? Smart contracts are a piece of code that is stored in a decentralized database (blockchain), and that changes the state of the database based on incoming transactions from other peers on the blockchain, this database lives in the nodes of the blockchain. The catch here is that there is no centralized entity that can change the state of the database, as all the transactions that trigger the computation of the smart contract are treated egalitarian. Moreover, the state change of the database (the ledger), is validated by all the nodes of the network, where this state change is pruned if these nodes can't reach a consensus on the incoming transaction. Hence, the nature of the smart contract eliminates the risk between two entities that want to perform an exchange, by transferring this risk to the smart contract's encapsulated code that lives on every node of the blockchain. Nonetheless, the nature of the smart contract also poses some drawbacks in its use case. A smart contract ensures correctness and availability but also ensures that the changes are publicly known for each node. Thus, if the concept of smart contracts would be implemented in a financial setting as governing and securing transactions between two parties, these transactions are publicly available given the premise that the blockchain is public (e.g. Ethereum, Bitcoin, Cardano). This creates a vacuum and utility for privacy that can be fulfilled by designing the blockchain as private, or semi-private. However, this scenario is counterintuitive as its neglect the decentralized nature of the blockchain but circumvents the disadvantage of the public openness and transparency of a fully permissionless blockchain.

Kasper Borgbjerg
kasperib@uio.no

References:

Greenspan, G. (2016, April 17). *Why many smart contract use cases are simply impossible*. CoinDesk Latest Headlines RSS. Retrieved April 30, 2022, from https://www.coindesk.com/markets/2016/04/17/why-many-smart-contract-use-cases-are-simply-impossible/

Delmolino, K., Arnett, M., Kosba, A., Miller, A., & Shi, E. (2016, February). Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab. In International conference on financial cryptography and data security (pp. 79-94). Springer, Berlin, Heidelberg.