Abstract

The use of oracles to send data that is external, into the blockchain is critical to the proper functioning of smart contracts deployed within a blockchain. The concept of oracles is an interesting development in the blockchain industry. In order to gain a proper understanding of the working of oracles, it is important to understand the state of the art in blockchain. This work consists of review of Bitcoin and Ethereum blockchain concepts. Bitcoin blockchain uses a design that implements decentralization and immutability to manage the bitcoin currency. Unlike Bitcoin that allows only simple operations to be performed to ensure security, Ethereum also allows code of complex nature to be executed on the blockchain. Further, we understand the QTUM blockchain eco-system that uses the best of both Bitcoin and Ethereum blockchains. QTUM provides a Turing-complete blockchain stack that can execute smart contracts and decentralized applications and, uses the Ethereum Virtual Machine (EVM). However, in contrast to Ethereum, QTUM is built upon Bitcoin's Unspent Transaction Output (UTXO) model and employs a Proof-of-stake consensus mechanism that is more scalable and practical for business adoption. A transaction in the blockchain consists of inputs and outputs. The outputs that have not been spent yet are referred to as UTXOs. We examine the various oracles currently available and categorises them as centralized and decentralized. We discuss in detail oracle systems such as Provable, Chainlink, TownCrier, Astrea and Augur. The work also explains implementations of smart contracts and oracles on the Qtum blockchain. An innovation from the existing implementations of oracles has also been designed, discussed and implemented which is a contribution to the literature on Oracles for blockchain.