

Abstract

In accordance with the invention there may be provided a method and corresponding system for controlling the performance of a process conducted via a blockchain. The blockchain may or may not be the Bitcoin blockchain. The process may be a lending process. Advantageously, the invention provides a mechanism which enables the ultimate owner of a property or other asset to borrow funds against that asset, and sets out how this can be achieved in a manner which does not require the return to the investor(s) to be determined through the payment of interest. This makes it compliant with non-interest forms of lending. The invention provides a blockchain-implemented method (and corresponding system) of embedding data in a blockchain transaction (Tx). The method comprises the steps of deriving a public-key-private key cryptographic pair for the data; deriving a signature for the data using the public key-private key cryptographic pair; codifying the data to generate codified metadata for the data. The codified metadata is transmitted to the blockchain in a transaction. A signature is received and a script from at least one user to enable access to the embedded data. The script comprises a public key of a signatory. The metadata comprises a hash of the data and a pointer to the data so that it can be located. The hash is used as a primary key in a lookup table where the data is stored.

Figure 1.