Abstract

The invention provides systems and methods for converting high level source code into an arithmetic circuit which represents the functionality expressed in the source code. The invention comprises a translation/interpretation component for performing this conversion. In a preferred embodiment, the source code is a smart contract such as those used in relation to a blockchain platform. The invention could be used in relation to the Bitcoin network, for example. A method in accordance with an embodiment comprises the steps of: processing a portion of high level source code (e.g. a smart contract) to generate an arithmetic circuit. The arithmetic circuit comprises one or more arithmetic gates arranged to represent at least some of the functionality expressed in the source code. The processing involves evaluating one or more constants provided in the source code to produce one or more expressions that include Boolean and/or arithmetic operators. The arithmetic circuit comprises n-bit wires connected to arithmetic gates; it can be used to provide a hardware and/or software circuit. The arithmetic circuit can be used to generate a quadratic program which can be executed upon a processor.

Figure 2.