

Smart contracts written in quasi-natural language, executed through simulated human reasoning

Overview

Smart contracts can vastly improve the efficiency and security of traditional contracts, through self-executing autonomy. The most prominent smart contract implementation is the Ethereum blockchain platform. Solidity is a contract-oriented language, designed to target this platform.

Whilst Ethereum is an enabling technology, challenges arise in encoding; it is difficult to program a smart contract to accurately capture all the desired contractual requirements. Encoding in Ethereum entails translating a natural language statement of a contract into an object-oriented code (in Solidity). There is thus a high chance of a loss in translation, and the gap between natural language and Solidity paradoxically introduces new errors and inefficiencies in the system. This is true even when the legal and programming skills reside in the same person implementing smart contracts. A novel language that aims to solve the problems with Solidity is presented here.

Technology

Researchers from Imperial College London have developed **Logic-based Production System (LPS)** which aims to unify many different computing paradigms. LPS has both:

- a) Logic programming rules, representing *'beliefs'*
- b) Reactive rules and constraints, representing *'goals'*

Programs in LPS have both a logical and computational interpretation. The logical interpretation makes them easier to understand, develop and maintain. The computational interpretation makes them easier to execute efficiently.

The representation of beliefs as logic programs in LPS is supported by psychological and normative studies of human reasoning, such as normative models. The representation of goals in LPS is supported by their similarity to production systems, which are one of the most widely accepted computational models of human thinking.

Applying LPS to smart contracts allows users to write code which very closely resembles natural language. It closes the translation gap currently present in smart contracts and makes it possible for lawyers to generate smart contracts intuitively and directly, without the need for an intermediary programmer. Furthermore, LPS is far more compatible with regulatory compliance requirements, as the monitoring and execution of actions is backed by the clear logical reading of the contract itself.

A prototype of LPS has been used to teach logic and computing to children, demonstrating its intuitiveness. The belief component of LPS has been used to formalise legislation, including sections of the British Nationality Act, thereby demonstrating its expressivity and utility. The goal component of LPS is an important addition, which allows LPS to regulate behaviour.

Benefits

- Simpler translation
- Greater compliance compatibility
- Reduced encoding time & resources needed

Alessandro Garcia

Technology Licensing Executive

e: alessandro.garcia@imperialinnovations.co.uk

t: +44 (0)20 3727 2059

w: www.imperialinnovations.co.uk

Technology reference number: 8380