Р. Е. СПИРИДОНОВ
Санкт-Петербургский государственный электротехнический университет
«ЛЭТИ» им. В.И. Ульянова (Ленина), Санкт-Петербург

RESTRICTED MOVE – ЯЗЫК ОПИСАНИЯ СМАРТ-КОНТРАКТОВ ДЛЯ СОЗДАНИЯ И УПРАВЛЕНИЯ ФИНАНСОВЫМИ АКТИВАМИ НА ОСНОВЕ БЛОКЧЕЙН ПЛАТФОРМЫ DFINANCE

Создание смарт-контрактов для выпуска токенов или управления другими цифровыми финансовыми активами в абсолютном большинстве существующих блокчейн платформ требуют знаний программирования на специфичном для конкретной платформы языке, что накладывает ограничение по привлечению финансовых специалистов с классических рынков.

В данной работе представлена концепция языка Restricted Move, позволяющего формировать описание смарт-контракта на финансовом английском языке, а также его дальнейшее развитие в расширяемый пользователями высокоуровневый язык управления цифровыми активами.

Введение. Впервые смарт-контракты были реализованы в блокчейн платформе Ethereum, как компилируемые в байт-код функции для EVM, сохраняемые внутри цепочки блоков и позволяющие выполнять различные действия по созданию пользовательских токенов [1]. Но ввиду сложности по их созданию – написание смарт-контрактов до сих пор остаётся недоступно широкому классу пользователей, ввиду сложности их организации, требования специфичных средств разработки и особенностей по их отладке. Отдельной проблемой стоит необходимость учитывать ряд задач по обеспечению должного уровня безопасности смарт-контрактов от взлома злоумышленниками с целью хищения средств или компрометации доступа к другим кошелькам. Также стоит обратить внимание на замкнутость блокчейн платформ внутри себя и на отсутствие их совместимости друг с другом в большинстве случаев, что делает невозможным выполнение операций между разными сетями без участия посредника, который не автоматизирован и требует человеческого участия.

Из всех вышеуказанных проблем вытекает необходимость в создании нового языка, доступного широкому классу пользователей, знакомым с финансовыми рынками и осознающими все возможности современных финансовых инструментов при их переложении в мир крипто валют и автоматизированного управления цифровыми активами. В качестве основы для такого языка предлагается выделение языка Restricted Move и его реализация в блокчейн платформе DFinance.

Требования к языку. Как и в любом высокоуровневом языке в Restricted Move можно выделить элементы языка: алфавит, синтаксис и правила оформления программы; организацию действий над данными: ввод-вывод данных, а также набор выражений для работы с данными; организацию самих данных. Но весь привычный набор, характеризующий язык программирования, в данном случае проблематичен к выделению, ввиду внешней простоты и близости по семантике к фразам описания финансовых инструментов на английском языке, а также из-за наличия неопределённости о размере всего множества элементов языка – язык должен иметь возможность дополняться новыми фразами и возможностями.

Рассмотрим несколько примеров описания, создающих новые токены, на финансовом английском языке:

Create 1 non-fungible Token as an American Call Option contract, representing 1 Nike Jordan Air, expiring November 30th.

Create 100 Tokens as an American Put Option contract, representing 100k USD each, balanced with 50% S&P, 25% European Sovereign Debt, 15% BTC and 10% Real Estate, not expiring.

В подобных примерах можно выделить типовые конструкции подзапросов, определяющих параметры создаваемого инструмента, а всю последовательность таких конструкций можно формализовать в виде последовательного вызова функций с указанием для них аргументов.

Для большего подобия естественным языкам следует позволить нарушать стандартную последовательность описания, обеспечив возможности по началу описаний с разных его частей, например, сначала описать ряд ограничений инструмента, а затем сам создаваемый инструмент.

Дополнительным требованием к Restricted Move является хранение всей структуры языка внутри цепочки блоков. Из этого требования вытекает ряд ограничений и возможностей по синтаксису языка. Например, при обновлении версий языка будет автоматически обеспечиваться обратная совместимость с предыдущими версиями.

Структура языка. Все части описания можно разделить на несколько видов блоков (*Nodes*): управляющие потоком вызовов функций – *Flow*, а также непосредственного заполнения данных для создаваемых инструментов – *Data*. Все блоки совместимы друг с другом, если не указаны дополнительные ограничения по их сочетанию друг с другом, помимо этого, целиком в запросе могут присутствовать взаимоисключающие вызовы, которые не должны находиться одновременно в одном смарт-контракте, что также необходимо предусмотреть в структуре данных каждого из блоков.

Data Nodes – узлы для заполнения данных в смарт-контракт. Возможны следующие варианты: ввод строки, ввод числа, выбор из списка значений, ввод даты. При этом у каждого из приведённых типов узлов могут быть указаны свои ограничения, добавляющие проверку введённых значений и накладывающие требования на их ввод.

Flow Nodes – узлы для управления потоком формирования смарт-контрактов. В простейшем варианте языка, достаточно двух видов узлов для последовательного и параллельного вызова следующих за ними блоков *Nodes*. Но для упрощения итоговых внутренних конструкций, также необходимо ввести тип потокового узла – множество, который является аналогом последовательного заполнения запроса, но не накладывает ограничений на следование начальному порядку перечисленных внутри него блоков. Так как в описаниях смарт-контрактов могут существовать аргументы, которые можно опустить и не указывать полностью, то и параллельный вызов следует также доработать, с помощью ввода в этот вид блока параметра *optional,* сигнализирующий о необязательности заполнения информации в элементы внутри этого блока.

Structure Nodes – узлы, определяющие структурные единицы для описания функций и последовательностей вызовов других блоков. По сути, каждый новый контракт будет являться *Structure Node,* описывающий череду вызовов других контрактов с указанием информации об их аргументах.

Заключение. Задача по созданию специального языка описания управляющих и декларативных смарт-контрактов для финансовой отрасли с хранением структур языка и предоставления возможности по его расширению из новых блоков с вызовами смарт-контрактов решаема. Перспективы развития подобного средства не ограничиваются текущим синтаксисом и позволяют предусмотреть дальнейшее развитие языка с добавлением в него блоков с интеллектуальным распознаванием фраз и разбором на вызовы отдельных языковых структур.

ЛИТЕРАТУРА

1. Vitalik Buterin. Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. 2013. URL {https://ethereum.org/en/whitepaper/}.

R.E. Spiridonov, (SPbETU “LETI”, St. Petersburg)

Restricted Move – Smart Contract Describing Language for Creating and Controlling of Financial Actives on DFinance Blockchain Platform

Smart contracts creation to issue tokens and to control of other digital financial actives mostly on all blockchain platforms require knowledge of programming language of specific platforms. This fact imposes a restriction on attracting financial specialists from classical markets.
In this paper the concept of Restricted Move language is presented. It allows users to form a smart contract description on financial English, as well as its further development into a high-level digital assets management language, which can be extended by users themselves.