СЕМАНТИЧЕСКИЕ СМАРТ-КОШЕЛЬКИ

Свириденко Дмитрий, д.ф.-м.н., профессор

Настоящая статья является логическим продолжением предыдущей статьи автора, посвященной семантическим «умным» контрактам, и, как было обещано, в ней пойдет речь об одном важном и весьма перспективном применении этого понятия в цифровой экономике – об ***электронных кошельках***. Но прежде чем начать обсуждение данной темы, кратко напомним еще раз основные положения концепции семантических смарт-контрактов.

Основной вывод предпринятого ранее анализа понятия «умного» контракта можно кратко сформулировать следующим образом – *вместо программирования смарт-контрактов предлагается их логико-вероятностное моделирование, при обязательном условии сохранения при этом семантики деловых контрактных отношений.* Заметим, что такая замена программирования на моделирование открывает принципиально иные возможности перед проектировщиками и пользователями семантических смарт-контрактов, позволяя:

- существенно расширить спектр деловых отношений, допускающих оформление в виде смарт-контрактов и сбалансированно учитывающих элементы доверительных отношений между партнерами, вынося при необходимости в интегрированные с системой распределенные реестры только ту информацию, которые жизненно необходима для обеспечения установленного партнерами уровня доверия, например, хранить историю изменений условий или структуры смарт-контракта;
- при проектировании и пользовании контрактами активно использовать широкий спектр логико-вероятностных методов и алгоритмов семантического моделирования, в том числе и алгоритмов искусственного интеллекта, что делает возможным эффективное управление исполнением контрактов, контролируя семантику формализуемых контрактом отношений, прогнозируя и планируя ход будущих событий;
- сделать контракты доступными для самостоятельного их проектирования, понимания и анализа специалистам, далекими от программирования, в том числе и юристам, решая, тем самым, проблему юридической верификации и легализации создаваемых смарт-контрактов,
- рассматривать семантические смарт-контракты как декларативное средство формализации деловых отношений агентов/акторов, т.е. интерпретировать их как обычные бизнес-процессы, что делает возможным легкую и естественную их интеграцию в деловую среду различной природы и сложности.

Важен тот факт, что предлагаемая концепция отделяет смарт-контракты от используемого при их исполнении того или иного распределенногго реестра.

Таких обслуживающих смарт-контракты реестров может быть несколько и выбор нужного должен определяться условиями и свойствами самого контракта, реализующего согласованный партнерами сценарий реализации механизма доверия.

Подводя итоги вышесказанному, можно сказать, что на **семантический смарт-контракт** наиболее целесообразно смотреть как на *логико-вероятностное представление некого бизнес-процесса, описывающего деловые отношения агентов/акторов, с возможными (но не обязательными) дополнительными мерами децентрализованного обеспечения доверия*. Заметим, что такая трактовка смарт-контрактов как обычных бизнес-процессов имеет то преимущество, что позволяет легко интегрировать смарт-контракты в деловую среду управления сложными объектами, допускающими их представление в виде системы взаимодействующих бизнес-процессов.

Вернемся к теме электронных кошельков. Для многих людей оплата покупок или услуг в магазинах, ресторанах и кафе пластиковыми карточками стала вполне привычным делом. Люди привыкли, что это вполне безопасно и удобно. Однако с появлением интернета и, особенно, мобильных гаджетов (смартфонов, коммуникаторов, планшетов и т.п.) и мобильного интернета этот процесс стал еще более удобным и выгодным – для этого следует лишь открыть так называемый *электронный* или *виртуальный кошелек* – некий аналог банковского счета, который также, как и банковский, можно пополнять, а цифровыми или электронными деньгами, хранящимися на нем, с помощью интернета расплачиваться за услуги и товары, перечислять цифровые деньги на другие счета и совершать другие операции. В настоящее время под **электронным кошельком** обычно понимается специальная программа, которая, используя коммуникационные возможности интернет, позволяет хранить и управлять электронными деньгами, выполняя разнообразные виртуальные расчеты. Другими словами, на электронный кошелек предлагается смотреть как на своеобразный инструмент, с помощью которого можно в удаленном режиме, находясь в сети интернет, напрямую и практически мгновенно управлять цифровыми денежными средствами: следить за своим балансом, оплачивать коммунальные платежи и услуги связи, а также пользование различными интернет ресурсами, совершать всевозможные онлайн-покупки, переводить средства с пластиковых карт на кошелек и обратно, оплачивать кредиты и прочее. Существуют электронные кошельки, способные управлять сразу несколькими виртуальными счетами, в том числе номинирован-ными в разных валютах - такие программы управления называют иногда *киперами***,** различая тем самым сами счета и называя именно их электронным кошельком, и программу управления этими счетами. При этом дистанционное управление счетом или несколькими счетами способно учитывать текущий баланс счета/ов, переводить титульные знаки, пополнять кошелек, выставлять счета, оплачивать покупки, переводя средства с кошелька на платежные реквизиты продавца или поставщика сервиса, совершать обмен средств**,** учитывать наличие бонусов, предлагаемых различными компаниями, места совершения покупки и т.д., и т.п., что делает электронный кошелек очень похожим по своему функционалу на банковский счет.

Тем не менее, следует отметить, что между банковскими и цифровыми счетами существуют определенные различия, дающие зачастую электронным кошелькам весомые преимущества. Например, *анонимность* - для создания электронного кошелька пользователям достаточно зарегистрироваться на сайте той или иной виртуальной платежной системы без предоставления каких-либо документов. Другим преимуществом является *круглосуточная доступность* кошелька. Кроме того, деятельность подобных платежных систем, в отличие от банковских, *бессрочна* и, как правило, за сервис *не надо платить*. Однако, если вы захотите вывести со своего кошелька цифровые деньги и превратить их в наличные или перевести на свой банковский счет, потребуется заплатить комиссионные и иногда немалые. А если речь идет о крупных суммах, то придется пройти и процедуру идентификации. Тем не менее, именно наличие указанных выше преимуществ явилось главной причиной исключительной популярности электронных кошельков. Как одно из следствий такой популярности явилось то, что наличные деньги во всем мире постепенно уступают место виртуальным, цифровым деньгам.

Естественно, что у электронных кошельков есть и недостатки. Например, до сих пор не все торговые или сервисные организации принимают к расчету цифровые деньги, хотя, с другой стороны, появились и сервисы, которые можно оплатить только с помощью кошельков или банковских карт. Заметим, что расчеты электронными деньгами обязательно требуют наличия доступа в интернет, что не всегда оказывается возможным. У пользователя могут возникнуть проблемы с доступом к кошельку при утере нужной для этого информации. И т.д., и т.п. Но самыми большими проблемами электронных кошельков являются вопросы их *функциональности, надежности, безопасности и юридической верифицируемости*.

В последнее время пользователи начинают предъявлять все более и более высокие требования к набору предоставляемых кошельком сервисов и «интеллекту» кошелька, что заставляет платежные системы и «финтеховкие» организации, борясь за клиентов, весьма активно работать в этом направлении. Явно прослеживается тенденция к созданию все более «умных» электронных кошельков или, как их еще называют, ***смарт-кошельков***: надежных, безопасных, многофункциональных и высоко «интеллектуальных». Эта тенденция еще больше усилилась в связи с появлением криптовалют.

Современные «продвинутые» электронные кошелки могут также предоставлять возможность пользоваться «***умным меню***», позволяющим покупателю оплачивать свои покупки по наиболее выгодному курсу, с учетом всех существующих и действующих скидок и бонусов в том или ином магазине, получать подсказки типа «какой карточкой и/или валютой выгоднее оплачивать покупку», планировать семейный бюджет; ставить финансовые цели для накоплений и осуществлять мероприятия по их реализации, планировать будущие платежи и поступления в календаре, синхронизировать их с различными компьютерными календарями, а также генерировать отчеты и графики, демонстрирующие пользователям их расходы/поступления по различным

категориями затрат, сравнивая их с прошлыми периодами и поставленным бюджетом («умная» статистика), формировать информационные напоминания о предстоящих платежах/поступлениях через различные коммуникационные каналы (USSD, SMS, e-mail, чат-боты мессенджеров) и т.д. Более того, подобные ***«умные» электронные кошельки*** способны в отдельных случаях сами принимать решения, в том числе и по выбору наиболее оптимальных вариантов оплаты, а также планировать/прогнозировать доходы и расходы.

Мы уже выше упоминали, что некоторые электронные кошельки позволяют пользователям «привязать» к нему несколько своих банковских карт с целью оптимизации совершения покупок определенного вида в зависимости от товара или места его приобретения. Более того, пользователь может также «открыть» несколько электронных кошельков и загрузить программу, которая**,** как и основные программы управления кошельками, позволит также распоряжаться средствами на этих кошельках. В некоторых электронных кошельках предусматривается возможность подключать для учета банковские счета из разных банков, что позволяет пользователю не вносить вручную данные о платежах, осуществляемых с использованием других банковских карт. Заметим также, что допускается интересная возможность нескольким владельцам открыть *совместный* электронный кошелек. В этом случае электронный кошелёк помогает разобраться с самой острой темой совместного владения – это прозрачность поступлений и расходов.

С появлением криптовалют роль и значение электронных кошельков возросла еще больше. У них, естественно, появились и новые функции. Так, например, одной из важных функций биткоин-кошелька BitX (доступен для мобильных пользователей Android и iOS) является то, что пользователи могут покупать и продавать цифровую валюту в самом приложении. Очевидно, что для начинающих трейдеров и неопытных пользователей такие мобильные биткоин-кошельки будут очень полезными, поскольку они могут делать все, что нужно, используя только одно приложение и не открывая специальные окна браузера для торговли. Этот кошелек называется **«***умным***»,** поскольку он позволяет изучать поведение пользователей и использовать эту информацию при организации торговли. Например, прогнозировать и планировать назначаемую кошельком цену комиссии транзакции, о чем речь пойдет ниже. Кстати, в недалеком будущем BitX планирует выпустить поколение виртуальных номеров кредитных карт для своего кошелька, чтобы с их помощью пользователи смогли бы тратить биткоины по всему миру.

Однако появление криптовалют и новых технологий, связанных с их продвижением и использованием, например, технологий *распределенных реестров*, породило и множество проблем, связанных с функционированием «умных» электронных кошельков, обслуживающих криптовалюты. Одной из таких проблем является проблема *зависания транзакций*. Поясним эту проблему на примере сети Биткоина.

Поскольку число транзакций в сети Биткоина в последние годы резко выросло, а майнеры из чисто прагматических соображений предпочитают включать в свои

блоки, прежде всего, транзакции с самой высокой комиссией, то сгенерированные пользователями транзакции с низкой или нулевой комиссией включались майнерами в блоки в последнюю очередь. Это привело к тому, что низко комиссионные транзакции стали постепенно накапливаться в «пулах памяти» (очередях транзакций), а на их подтверждение требовались уже часы, дни и даже недели. Появились случаи, когда такие транзакции и вовсе не подтверждались. Таким образом, изначально предполагаемая комиссия в размере одного *сатоши* (0.00000001 BTC) стала часто недостаточной, хотя, вообще говоря, и этот размер комиссии в некоторых случаях представляется излишне высоким, что, например, делает не рентабельным использования биткоина как платежного средства в Интернет вещей.

Стандартная рекомендация для пользователей сети Биткоина – при желании быстрого исполнения транзакции дать распоряжение своему кошельку включить более высокую комиссию. Такое указание может быть дано вручную загодя или при отправке транзакции. При этом рекомендации по настройке комиссий можно получать из самых разных источников (смотри, например, 21.co). Существуют кошельки, которые могут автоматически поддерживать так называемые *динамические комиссии.* Такие «умные» кошельки сами рассчитывают комиссии, достаточные для включения транзакции в ближайший или один из ближайших блоков. Кроме того, они способны выбрать размер комиссии в зависимости от приоритета и времени проведения транзакции.

Кроме повышения размера транзакции можно воспользоваться приемом «*перепрыгивания очереди*», используя для этого опцию «возможной замены по комиссии» (Opt-In Replace-by-Fee, или Opt-In RBF), что позволяет повторно отправить в сеть ту же транзакцию, но уже с более высокой комиссией. Эту опцию поддерживают два кошелька: Electrum и GreenAddress. Заметим, что, хотя и не все майнеры поддерживают Opt-In RBF, большинство узлов Биткойна все-таки принимают новую транзакцию вместо старой и позволяют ей встать в начало очереди. Еще один способ ускорить прохождение транзакции – применить прием «*ребёнок платит за родителя*» (Child Pays for Parent, или CPFP). Суть метода состоит в том, чтобы воспользоваться тем обстоятельством, что майнеры, как правило, выбирают группу транзакций с самой высокой *суммарной* комиссией.

«Умные» криптовалютные кошельки (смотри, например, биткойн-кошельки Airbitz, Copay, Mycelium, Electrum, GreenAddress и Coinom), помимо определения размера комиссии для транзакции, способны не только расплачиваться за ежедневные покупки и услуги, но могут поддерживать разные альткоины и токены, позволяют создавать общие кошельки с мультиподписью, не требуя при этом дополнительной регистрации, дают возможность экспортировать приватные ключи, а затем импортировать их в новый кошелёк и сразу же с него проводить транзакции. Некоторые кошельки позволяют использовать *сдачу* в следующей транзакции, получаемую от предыдущей транзакции при ее проведении

До сих пор мы говорили о функциональности кошельков, отправляющих транзакции. Не менее интересные стратегии поведения реализованы и в кошельках *получателей.* Например, такие кошельки могут ограничивать

получение денежных средств теми или иными условиями или поддерживать расходование еще неподтверждённых транзакций. В отдельных случаях кошелек может спросить отправителя, хочет ли он использовать тот или иной прием для ускорения транзакции или порекомендовать ему конкретный прием.

Ранее мы уже говорили о преимуществах электронных кошельков. Напомним, что основное их преимущество заключается в исключительной *мобильности и скорости* осуществления электронных платежей – платеж может быть осуществлен практически мгновенно и в любом месте, где есть интернет, например, в спокойной, домашней обстановке. Другое преимущество электронных кошельков, о котором частично шла речь выше – это *анонимность* операций с электронными деньгами, а также отсутствие *проблемы ликвидации* кошелька и/или его *переоформления.* Ну, и еще одно немаловажное достоинство электронных кошельков – это практически *круглосуточная* доступность осуществляемых ими сервисов.

Как видно из вышесказанного, современные электронные кошельки представляют из себя конструкции с весьма развитой *функциональностью* и достаточно сложной *логикой* принятия решений. И это при том, что исполняемые ими собственно расчетные операции в тоже время носят весьма *ограниченный* и *примитивный* характер. Данное обстоятельство делает электронный смарт-кошелек чрезвычайно интересным и почти идеальным объектом его формального представления в виде декларативной исполнимой *семантической модели*, используя для этого соответствующий логико-вероятностный инструментарий, о котором шла речь в статье автора про смарт-кошельки. Но естественно возникает вопрос – а какое преимущество даст нам подобный подход?

Чтобы ответить на этот вопрос вернемся к анализу имеющихся недостатков электронных кошельков. Ранее мы уже отмечали некоторые их них. Но главным недостатком, по мнению автора, является то, что потенциальный или действующий владелец кошелька, как правило, лишен возможности самостоятельного конструирования нужного ему кошелька или модернизации существующего. Поэтому, прежде чем открыть электронный кошелек, пользователю необходимо осуществить поиск с тем, чтобы тщательно проанализировать и затем выбрать именно ту платежную систему, которая в наибольшей степени отвечала бы его потребностям и требованиям - какие способы пополнения кошелька предлагает платежная система (заметим, что большинство кошельковых сервисов предлагают перевести деньги на кошелек со счета мобильного телефона, пополнить счет через банкомат или платежный терминал, произвести почтовый или банковский перевод, воспользоваться интернет-банкингом), какую комиссию она назначает за осуществление отдельных операций, например, за перевод на банковский счет, какие дополнительные сервисы может предложить кошелек и т.п. При этом понятно, что выбор той или иной платежной системы связан с определенным риском – какова легитимность платежной системы, каков ее рейтинг на рынке, действительно ли присутствует обещанная «умная» функциональность кошелька и т.п. Могут быть вопросы и к юридической обоснованности тех или иных сервисов кошелька и их надежности, а

также к защите кошелька от несанкционированного доступа. Как показывает опыт, риски резко возрастают, если речь идет о криптовалютных кошельках, особенно, если они открываются в платежных системах, базирующихся на технологии распределенных реестров. Естественно возникает вопрос – есть ли способ преодолеть все эти препятствия? Ответ на этот вопрос и дает концепция семантических смарт-контрактов и основная декларируемая здесь идея заключается в том, что электронный кошелек предлагается рассматривать как ***семантический смарт-контракт****, который заключает/ют сам/и с собой его владелец/цы и его создание или модернизация осуществляется в рамках и средствами некой единой платформы.*.

Как представляется автору, главным достоинством такого подхода является возможность потенциальному владельцу в рамках некой единой платформы, используя простые и понятные инструменты семантического моделирования, либо самому создавать смарт-кошелек с нужным ему сервисом, либо выбрать из ряда уже существующих шаблонов кошельков наиболее походящий и настроить его (удаляя или создавая отдельные сервисы, либо модифицируя логику («интеллект») кошелька таким образом, чтобы функциональность кошелька, его «интеллектуальность» и иные свойства наиболее полно удовлетворяли бы желаниям и требованиям владельца. Подобный семантический смарт-кошелек, рассматриваемый как частный случай семантического умного контракта, когда владелец/цы выбираемого, создаваемого или модернизируемого кошелька заключает/ют контракт с самим/и собой, способен будет способен осуществлять автоматизированное исполнение следующих функций:

- Роботизированное управление счетами отдельного кошелька, принадлежащего одному владельцу (заметим, таких счетов у кошелька может быть несколько);
- Роботизированное управление счетами отдельного кошелька/ совместного мультивалютного кошелька, принадлежащего нескольким владельцам;
- Роботизированное управление некой совокупностью кошельков, принадлежащих одному или нескольким владельцам; при этом могут предусматриваться ситуации активизации других кошельков и/или генерации новых кошельков и/или закрытие существующих при определенных условиях.

Заметим, что во всех вышеуказанных случаях должны решаться задачи:

- квазиоптимального управления отдельным кошельком (счетами кошелька) по различным критериям;
- квазиоптимального управление совокупностью кошельков по различным критериям;
- планирования и прогнозирования (на основании истории «поведения» кошелька/ов, учета внешнего окружения, вложенных в кошелек или сгенерированных кошельком/ами стратегий и т.п.; заметим, в частности, что семантический «умный» кошелек может решать задачу осуществления

заданных или сгенерированных им самим рекуррентных платежей);

- Надежной защиты кошелька от несанкционированного проникновения;
- Интерактивного иформационного обслуживания владельца/ов кошелька/ов (возможно, рассматривая владельца/другой кошелек/внешний мир как *оракул*), умная статистика и т.п.
- Прочие «умные» функции.

.