УДК 004:338

ДИЗАЙН-МЕХАНИЗМ ТОРГОВЛИ ЭЛЕКТРОЭНЕРГИЕЙ В ДЕЦЕНТРАЛИЗОВАННОЙ ЭНЕРГЕТИЧЕСКОЙ СЕТИ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ СМАРТ-КОНТРАКТОВ

Белкин П.А., Ростовский Н.С.

Национальный исследовательский ядерный университет «МИФИ», Москва, e-mail: info@mephi.ru

Механизм торговли электроэнергией в децентрализованной энергетической сети с использованием технологии смарт-контрактов широко рассматривается в мире. В отличие от сделок с традиционными физическими товарами или услугами, торговля электроэнергией (особенно полученной от возобновляемых источников) обладает рядом отличительных свойств: нестационарностью генерации, невозможности хранения (или ограниченными возможностями), возможностью сбоев в поставках из-за того, что сам процесс торговли растянут во времени. В этой статье рассматривается проблема подтверждения достоверности сделок по торговле электроэнергией в условиях децентрализованной энергетической сети без участия посредников с использованием смарт-контрактов и технологии блокчейн с целью создания таких рыночных условий, в которых честное сотрудничество покупателя и продавца является наиболее выгодным поведением. В качестве дизайна такого механизма рассматривается использование двойного депозитного торгового протокола, который использует двусторонние платежные депозиты в сочетании с простыми криптографическими примитивами, и который может быть реализован с использованием смарт-контракта. Процесс торговли электроэнергией рассматривается в виде развернутой формы игры. Основным результатом является нахождение единственного равновесия или исхода с нулевой суммой, при котором выигрыш обоих игроков максимален.

Ключевые слова: смарт-контракт, децентрализованная энергетическая сеть, дизайн-механизмы, блокчейн, цифровая энергетика, блокчейн-платформы, возобновляемые источники энергии, децентрализованное управление, потребление электроэнергии, торговля энергией

ELECTRICITY TRADING DESIGN-MECHANISM IN A DECENTRALIZED ENERGY NETWORK USING SMART CONTRACT TECHNOLOGY

Belkin P.A., Rostovskiy N.S.

National Research Nuclear University MEPhI, Moscow, e-mail: info@mephi.ru

The mechanism for trading electricity in a decentralized energy network using smart contract technology is widely considered in the world. Unlike transactions with traditional physical goods or services, trade in electricity (especially from renewable sources) has a number of distinctive properties: unsteady generation, inability to store (or limited capabilities), the possibility of supply disruptions due to the fact that the trading process is stretched in time. This article discusses the problem of confirming the reliability of electricity trade transactions in a decentralized energy network without the participation of intermediaries using smart contracts and blockchain technology in order to create market conditions in which honest cooperation between the buyer and the seller is the most profitable behavior. The design of such a mechanism is the use of a double deposit trading protocol, which uses bilateral payment deposits in combination with simple cryptographic primitives, and which can be implemented using a smart contract. The process of trading in electricity is seen as extended form of the game. The main result is finding a single equilibrium or zero-sum outcome, at which the winnings of both players are maximized.

Keywords: smart contract, decentralized energy network, design mechanisms, blockchain, digital energy, blockchain platforms, renewable energy sources, decentralized management, electricity consumption, energy trade

Механизм торговли электроэнергией в децентрализованной энергетической сети с использованием технологии смарт-контрактов широко рассматривается в мире [1]. В отличие от сделок с традиционными физическими товарами или услугами торговля электроэнергией (особенно полученной от возобновляемых источников) обладает рядом отличительных свойств: нестационарностью генерации, невозможностью хранения (или ограниченными возможностями), возможностью сбоев в поставках из-за того, что сам процесс торговли растянут во времени. Основной задачей в таком случае является обеспечение взаимного доверия между сторонами на протяжении всего срока предоставления услуг. Продавец должен верить, что покупатель заплатит, а покупатель

должен верить, что продавец окажет услугу в полной мере, оговоренной в контракте. Традиционно эта проблема решается путем использования доверенных третьих сторон, таких как компании-эмитенты кредитных карт, компании-медиаторы, предоставляющие эскроу-счета, репутационные системы или судебное решение.

Для того чтобы убрать из системы доверенных третьих сторон или медиаторов, необходимо наложить ограничения на поведение соответствующих агентов. В рамках блокчейн-платформы существует программный способ обработки и регулирования транзакции, условия проведения которой участники предлагают автономно. Такие механизмы называются смарт-контрактами [2].

Тем не менее, основываясь на последних результатах применения данной технологии к сделкам по торговле электроэнергией [3], можно сделать вывод, что участники продолжают опираться на посредничество третьей стороны для гарантии соблюдения условий сделки [4]. Это означает, что, несмотря на рост использования блокчейн-платформ как средства отправки платежей без доверенных третьих сторон, важной проблеме предоставления распределенных во времени услуг уделено недостаточное внимание.

Возможным решением проблемы доверия между покупателем и продавцом электроэнергии является использование цифрового смарт-контракта, который публикуется в сеть продавцом, а покупатель инициирует исполнение данного контракта, причем правила смарт-контракта требуют, чтобы и продавец, и покупатель внесли гарантирующий депозит в смарт-контракт до совершения сделки, которые возвращаются им только в случае успешной торговли.

В данной работе проведено описание дизайна данного механизма с использованием инструментария теории игр, которое часто применяется в анализе механизмов, использующих блокчейн [5]. Основным результатом является нахождение единственного равновесия по Нэшу.

Целью исследования, проводимого в данной работе, является анализ экономических и технических механизмов, позволяющих снизить риски торговли электроэнергией в децентрализованной сети.

Материалы и методы исследования

Краткое описание процесса торговли электроэнергией в децентрализованной энергетической сети

Процесс торговли электроэнергией в децентрализованной системе происходит напрямую между двумя агентами: Покупателем и Продавцом.

Для совершения транзакции, в рамках которой Продавец продаст покупателю энергию, требуется совершить две операции:

доставка энергии: Продавец предоставляет потребителю электроэнергию в течение оговоренного в контракте периода времени. Сам временной интервал технически разбивается на более малые промежутки для фиксации результатов поставки и совершения торговли;

оплата энергии: Покупатель совершает платеж в пользу Продавца дискретным способом. Общая сумма платежа разбита по техническим интервалам торговли, и платежи осуществляются по факту поставки.

В любой торговой платформе одна из этих операций совершается первой. В нашем случае первой операцией является именно доставка энергии.

Описание механизма Предположения

1. Покупатель знает значение хеш-функции от $d - h(d)$, которое он может использовать для проверки правильности полученного количества энергии. Механизм шифрования зашит в логику платформы.

2. У Продавца и Покупателя есть пара асимметричных ключей, а их открытые ключи известны друг другу. Все продавцы знают открытые ключи всех покупателей.

3. Комиссионные за транзакции, связанные с развертыванием смарт-контракта и отправкой сделки с ним, малы по сравнению с ценой за единицу энергии.

Процесс поставки энергии с использованием двойного депозитного торгового протокола

Процесс торговли электроэнергией разбит на временные интервалы в рамках общего срока исполнения договора. Описываемый далее процесс применим в рамках каждого из этих интервалов по отдельности. В случае неизменности условий договоренности на следующем временном интервале нижеописанный процесс поставки электроэнергии и ее оплаты повторяется.

Все описанные в данном разделе механизмы обеспечиваются средствами блокчейн-платформы.

Ее основными функциями являются: создание цифровых кошельков участников; регистрация сделок; резервирование средств в процессе проведения и валидации сделки; автоматическое списание средств с кошельков участников сделок; рейтингование участников по степени их добросовестности в сделках; отключение недобросовестных участников от сети; выбор узлов, занимающихся проверкой транзакций.

Процесс поставки энергии конечному потребителю в рамках каждого интервала разбивается на следующие шаги (рис. 1).

Шаг 1. Действия Продавца: для каждой продажи Продавец будет публиковать новый смарт-контракт, который включает следующее:

- P_d : цена на электроэнергию;
- $h(d)$: хеш от планируемого к поставке количества электроэнергии;
- ID: идентификатор контракта, который генерирует платформа для однозначного определения данной сущности в системе;
- E_s : депозит в смарт-контракт в качестве страхования рисков для Покупателя;
- дополнительные параметры.

Рис. 1. Дизайн процесса торговли в децентрализованной системе с использованием двойного депозитного торгового протокола

Шаг 2. Действия Покупателя: Покупатель дополняет смарт-контракт. Он должен:

- подтвердить P_d – цену электроэнергии, заполнив тем самым адрес, кому будет организована доставка;

- внести депозит – E_b в смарт-контракт в качестве подтверждения намерения покупки.

Шаг 3. Доставка. Продавец отправляет зашифрованную версию d (количества отправленной энергии), а именно $enc_{v_{pub}}(enc_{k_{pri}}(d, ID))$, заинтересованному покупателю, где $enc_{v_{pub}}$ – хэш-функция с использованием открытого ключа v_{pub} покупателя, а $enc_{k_{pri}}$ – хэш-функция с использованием закрытого ключа k_{pri} продавца.

Шаг 4. Принятие/отказ доставки. Покупатель расшифровывает данные d , затем шифрует их, чтобы проверить, соответствует ли новый хеш ранее известному $h(d)$. Затем Покупатель предоставляет ответ.

Шаг 5. Согласование. Этот шаг выполняется после предыдущего и зависит от решения, принятого Покупателем.

Анализ ситуации с точки зрения теории игр

С учетом описанного выше дизайна механизма найдем равновесие по результатам анализа исходов данной игры.

Введем следующие обозначения:

$Ч, Ч'$ – честное поведение продавца и покупателя соответственно;

$Ф, Ф'$ – фальсификация данных Покупателем и Продавцом. Для Продавца это означает, что им была отправлена неверная информация, подписанная его ключом, для Покупателя же это означает оспаривание транзакции, отправка в сеть отличной от опубликованной Продавцом информации;

$М, М'$ – предоставление данных, которые невозможно расшифровать (мусор) Продавцом и Покупателем соответственно. Это соответствует тому, что Продавец отправляет строку, которая не может быть расшифрована с помощью соответствующего открытого ключа в Шаге 3, или Покупатель делает это в Шаге 4.

$ТВ X$ – терминальная вершина, или исход игры. X – порядковый номер.

$НД$ – ответ от Покупателя отсутствует.

Схематично описание торговли может быть представлено в виде игрового дерева, изображенного на рис. 2.

Описание возможных сценариев

Представим возможные сценарии взаимодействия между Покупателем и Продавцом и их исходы в виде таблицы.

Здесь T_s, T_b – комиссия, взимаемая сетью с Продавца и Покупателя соответственно, E_s, E_b – депозит Продавца и Покупателя соответственно, $Enrg', Enrg'', Enrg$ – реальный объем энергии, поставленный Продавцом и полученный Покупателем. $Enrg$ является целевым показателем поставки по контракту.

Номер строки таблицы соответствует порядковому номеру терминальных вершин, изображенных на рис. 2.

Сотрудничество нечестным образом со стороны Продавца (вершины 1-3) оказывается выгодным для него только в случае, если Покупатель принимает его сторону и подтверждает сделку. Однако при этом он теряет свой первоначальный депозит и получает меньшее количество энергии. Получается, что Покупатель переплачивает, и такое сотрудничество для него невыгодно. В случае нечестной игры Продавца ему выгоднее сообщить об этом сети, увеличив тем самым свой рейтинг, и вернуть депозит.

Рис. 2. Игровое дерево двойного депозитного торгового протокола

Исходы различных сценариев взаимодействия Покупателя и Продавца

Номер терминальной вершины	Продавец						Покупатель						Сеть	
	Депозит (возврат)	Оплата	Поставка энергии	Комиссия сети	Депозит (взнос)	Изменение рейтинга в сети	Депозит (возврат)	Оплата	Поставка энергии	Комиссия сети	Депозит (взнос)	Изменение рейтинга в сети	Депозит (остаток взноса)	Комиссия сети
1	Es	Pd	-Enrg'	-Ts	-Es	const	O	-Pd	+Enrg''	-Tb	-Eb	fall	Eb	+Ts+Tb
2	Es	O	-Enrg'	-Ts	-Es	const	O	O	+Enrg''	-Tb	-Eb	fall	Eb	+Ts+Tb
3	O	O	-Enrg'	-Ts	-Es	fall	Eb	O	+Enrg''	-Tb	-Eb	rise	Es	+Ts+Tb
4	O	O	-Enrg'	-Ts	-Es	const	O	O	+Enrg''	-Tb	-Eb	fall	Es+Eb	+Ts+Tb
5	O	O	-Enrg'	-Ts	-Es	const	O	O	+Enrg''	-Tb	-Eb	fall	Es+Eb	+Ts+Tb
6	O	O	-Enrg'	-Ts	-Es	fall	Eb	O	+Enrg''	-Tb	-Eb	rise	Es	+Ts+Tb
7	Es	Pd	-Enrg	-Ts	-Es	rise	O	-Pd	+Enrg	-Tb	-Eb	fall	Eb	+Ts+Tb
8	Es	O	-Enrg	-Ts	-Es	rise	O	O	+Enrg	-Tb	-Eb	fall	Eb	+Ts+Tb
9	Es	Pd	-Enrg	-Ts	-Es	rise	Eb	-Pd	+Enrg	-Tb	-Eb	rise	O	+Ts+Tb

Выброс мусорной строки со стороны Продавца (вершины 4-6) всегда невыгоден, поскольку Продавец всегда теряет поставляемую им энергию, а в случае если будет честным Покупатель, то и свой рейтинг.

Честное сотрудничество со стороны Продавца (вершины 7-9) оказывается выгодным во всех случаях. Для Покупателя же игра в стратегии, отличные от честной, невыгодна с той точки зрения, что он получает всю энергию, но при этом переплачивает. Таким образом, выгоднее играть честно.

Результаты исследования и их обсуждение

Депозит или остаток взноса можно рассматривать, как итоговую сумму игры. Она получается равной нулю (игра с нулевой суммой) только в одном случае, когда оба участника сыграли честную стратегию. Это

и есть единственное равновесие при таком дизайн-механизме торговли.

Безопасность и жизнеспособность игры обеспечена наличием уникальной игры с положительными выплатами для обоих агентов, что гарантирует безопасность механизма. Увеличивая вес депозитов, мы можем усилить сдерживающий фактор.

В соответствии с предложенным механизмом игроки заинтересованы в продвижении в торговле из-за возможности увеличения стоимости депозитных сумм, зафиксированных в смарт-контракте.

Заключение

В данной работе был представлен дизайн-механизм торговли электроэнергией в виде двойного депозитного торгового протокола, как инструмент предотвращения мошеннических платежных операций и га-

рантии доставки между двумя участниками сделки на поставку электроэнергии, основанные на анализе дерева игрового взаимодействия между Продавцом, Покупателем и самим смарт-контрактом.

Основное предположение, сделанное в этой работе, заключается в том, что расчет по операциям происходит роллерно, а именно несколько раз в рамках промежутка времени поставки, обозначенного в контракте. Таким образом, единовременный объем средств, зачисленных в качестве депозита, невелик по отношению к стоимости роллерных сделок.

Рассмотренный дизайн механизма может быть автоматизирован с использованием технологии смарт-контрактов и блокчейна [6]. Эта технология позволит обеспечить необходимый уровень безопасности и прозрачности проведения сделок.

Список литературы

1. Белкин П.А., Ростовский Н.С., Посмаков Н.П. Применение технологии блокчейн в электроэнергетике как

связующей цифровой технологии при переходе на децентрализованную генерацию // Современные наукоемкие технологии. 2020. № 3 С. 19–24.

2. Melanie Swan. Blockchain. Blueprint for a new economy. Q'Reilly Media. 2015. 149 p.

3. Merlinda Andoni, Valentin Robu, D.Flynn, Simone Abram, Dale Geach, David Paul Jenkins, Peter McCallum, Andrew Peacock. Blockchain technology in the energy sector: A systematic review of challenges and opportunities. ResearchGate. [Electronic resource]. URL: https://www.researchgate.net/publication/328760651_Blockchain_technology_in_the_energy_sector_A_systematic_review_of_challenges_and_opportunities (date of access: 07.06.2020).

4. David Livingston, Varun Sivaram, Madison Freeman, and Maximilian Fiege. Applying Blockchain Technology to Electric Power Systems. Discussion Paper. Council on Foreign Relations. [Electronic resource]. URL: https://cdn.cfr.org/sites/default/files/report_pdf/Discussion_Paper_Livingston_et_al_Blockchain_OR_0.pdf (date of access: 07.06.2020).

5. Liu Ziyao, Nguyen Cong, Wang Wenbo, Niyato Dusit, Wang Ping, Liang Ying-Chang, Kim Dong. A Survey on Applications of Game Theory in Blockchain. ResearchGate. [Electronic resource]. URL: https://www.researchgate.net/publication/331429224_A_Survey_on_Applications_of_Game_Theory_in_Blockchain (date of access: 07.06.2020).

6. Jackson Ng. Smart Contract Escrow DApp – Buyer View. Medium. [Electronic resource]. URL: <https://medium.com/coinmonks/smart-contract-escrow-dapp-buyer-view-24f0b9bdb3a0> (date of access: 07.06.2020).