

УДК 336.743:004

<https://doi.org/10.31498/2225-6407.17.2018.146818>

## ОЖИДАЕМЫЕ И РЕАЛЬНЫЕ РИСКИ В БЛОКЧЕЙН-ТЕХНОЛОГИЯХ

<http://orcid.org/0000-0002-8423-2663>

**Волошин Вячеслав Степанович**, Ректор Приазовского государственного технического университета, заслуженный деятель науки и техники Украины, доктор технических наук, профессор, академик Академии экономических наук Украины.

**Vyacheslav Voloshin**, Rector of the "Priazovskiy State Technical University", Honored Worker Scientist of Ukraine, doctor of technical sciences, professor, academician of the Academy of Economic Sciences of Ukraine.

### *V. Voloshyn. Anticipated and real risks in block-chain technologies.*

*The article represents a review of problems and risks and the prospects of development in the domain of block-chain technologies. The article contains the available data regarding the degree of distribution of block-chain technologies as a contemporary and widespread commodity product. It was noted that the projects of application of block-chain technologies are widely discussed and realized throughout the world. They are based on the opportunities of this computer product, due to its qualities, like reliability universality and the absence of mediator. Analyzed were the risks, connected with application of this product, including objective, generally acknowledged and subjective ones, doing harm to development of the block-chain production. On the basis of represented expert evaluation the arguments were obtained for the prospects and risks due to application of this new technology. The groups of most probable reasons hampering widespread distribution of block-chain technologies beside the financial sphere were revealed. The work can be the subject of more detailed research in this field as a ground for objectification of risks and the means of popularization of up-to-date information technologies. The article could be of use for companies which are consumers of block-chain technologies in their applied direction and try to minimize their possible risks, due to their mastering the new high-tech consumer product. The conclusion was made that the existing actual and potential risks in known technologies of block-chain are far from being a sentence, being an opportunity of eventual finding solutions to such problems and preventing their influence on innovative processes in the society and ensuring man's safety in our quickly changing world.*

### **Волошин В. С. Ожидаемые и реальные риски в блокчейн-технологиях.**

*В статье сделан обзор проблем и рисков, а также перспектив развития в сфере блокчейн-технологий. В работе представлены доступные данные о распространенности блокчейн-технологий в качестве современного и популярного товарного продукта. Отмечено, что сегодня в мире активно обсуждаются и реализуются проекты применения технологий блокчейна. В основе стоят возможности этого компьютерного продукта, которые связаны с такими его качествами, как надежность, универсальность и отсутствие посредника. Рассмотрены некоторые риски, связанные с применением этого продукта, в том числе, объективные, общепризнанные и субъективные, наносящие вред собственно развитию блокчейн-продукции. На основании представительной экспертной оценки получены аргументы относительно перспектив и рисков, связанных с применением новой технологии. Выявлены группы наиболее реальных причин, тормозящих широкое распространение блокчейн-технологий помимо финансовой сферы. Работа может служить основанием для более тщательных исследований в этой области, как повод для объективизации рисков и пропаганды развития современных информационных технологий. Работа может быть полезной компаниям-потребителям блокчейн-технологий в прикладном их направлении, которые стремятся минимизировать свои риски, связанные с освоением нового высокоинтеллектуального товарного продукта. Сделан вывод, что существующие реальные и потенциальные риски в известных технологиях блокчейна - это не приговор, но возможность в будущем найти решение этих проблем, предупредить их влияние на инновационные процессы в обществе, обеспечить безопасность человека в нашем стремительно меняющемся мире.*

### **Волошин В. С. Очікувані та реальні ризики в блокчейн-технологіях.**

*У статті зроблено огляд проблем і ризиків, а також перспектив розвитку в сфері блокчейн-технологій. В роботі представлені доступні дані про поширеність блокчейн-технологій в якості сучасного і популярного товарного продукту. Відзначено, що сьогодні в світі активно обговорюються і реалізуються проекти застосування технологій блокчейна. В основі стоять можливості цього комп'ютерного продукту, які пов'язані з такими його якостями, як надійність, універсальність і відсутність посередника. Розглянуто деякі ризики, пов'язані із застосуванням цього продукту, в тому числі, об'єктивні, загально визнані і суб'єктивні, що завдають шкоди власне розвитку блокчейн-продукції. На підставі представницької*

експертної оцінки отримані аргументи щодо перспектив і ризиків, пов'язаних із застосуванням нової технології. Виявлено групи найбільш реальних причин, що гальмують широке поширення блокчейн-технологій крім фінансової сфери. Робота може служити підставою для більш ретельних досліджень в цій області, як привід для об'єктивізації ризиків і пропаганди розвитку сучасних інформаційних технологій. Робота може бути корисною компаніям-споживачам блокчейн-технологій в прикладному їх напрямку, які прагнуть мінімізувати свої ризики, пов'язані з освоєнням нового високоінтелектуального товарного продукту. Зроблено висновок, що існуючі реальні і потенційні ризики в відомих технологіях блокчейна - це не вирок, але можливість в майбутньому знайти рішення цих проблем, попередити їх вплив на інноваційні процеси в суспільстві, забезпечити безпеку людини в нашому стрімко мінливому світі.

**Постановка проблеми.** Появившиися благодаря сетям Интернет возможности для суперкоммуникаций там, где ранее они были просто невозможны, не только упростили человеческое общение, но привнесли элементы коммуникативности, которые ранее были неприменимыми как незэтичные, опасные для жизни, запрещенными по причинам криминала и т. д. Многие исследователи обращали внимание на эти негативные стороны сетевого общения и предрекали ему определенные угнетающие трансформации.

Но возможно, именно бесконечное сетевое общение стало предпосылкой появления пятой вычислительной парадигмы в виде технологий блокчейна, которые по своей универсальности и уникальности обещают стать в обществе некоторым функциональным сетевым продуктом нового универсального поколения. Ради этого, видимо, можно смириться и с четвертой, одной из последних на сегодня суперкоммуникационных информационных парадигм.

Далее все идет по спирали.

Сегодня в мире активно обсуждаются и реализуются проекты применения технологий блокчейна. В основе стоят возможности этого компьютерного продукта, которые связаны с такими его качествами, как надежность, универсальность и отсутствие посредника. Можно обобщить: технологии блокчейна применимы там, где имеются любые дискретные материальные потоки и где до этих технологий существовала необходимость в некотором *операторе, принимающем на себя посреднические функции* между поставщиком и потребителем. Поэтому реальные и субъективные риски становятся определенным препятствием на пути распространения современных технологий в различных отраслях бизнеса и хозяйства.

**Состояние вопроса.** Напомним, что, в некотором приближении, блокчейн-операция - это многофункциональная информационная технология учета некоторых обобщенных активов, например, регистрация движения дискретного материального потока между участниками определенной группы, каждый член которой обладает вполне конкретной, но обезличенной и неизменяющейся информацией о всех транзакциях внутри этой группы. Регистрации таких транзакций являются вполне объективными и независимыми от внешнего проникновения и осуществляются без какого-либо посреднического исполнения. В учетной основе блокчейн-операции находится алгоритм, сжимающий каждый актив любого размера до короткого кода из 64 символов (ХЕШ), который становится уникальным для данного документа, однозначно идентифицирует его для пользователей, но не восстанавливает исходную информацию и не позволяет ее изменять после т. н. майнинга. Такое определение технологий блокчейна весьма общо, но для наших целей в этой работе вполне применимо, так как позволяет найти общие признаки для возможностей их широкого использования.

Технология, которая вначале стала основой для появления целой области так называемых "виртуальных валют" уже сегодня находит широкое применение, в том числе, вне финансовых систем (табл. 1), как новая организационная парадигма для организации и учета активов в любом виде человеческой деятельности. Главные ее условия:

- наличие достаточной группы потребителей, которые не хотят зависеть от посредника;
- отсутствие единого управляющего центра (децентрализация);
- единственность записываемых данных и отсутствие возможности копирования.

Таблица 1.

## Области применения технологий блокчейн кроме финансовой

№№	Область применения	Компании	Примечание
1.	Изменения в банковской индустрии устранением многих посреднических операций	"Goldman Sachs" (США), UBS (Швейцария)	Работает
2.	Всемирная система внедокументальной идентификации личности на базе платформы Microsoft Azure	Компания "Microsoft"-проект ID2020. Компании "Avanade" и "Accenture"	Проект
3.	Управление торговлей недвижимостью	Crypto Realty Group, платформа "Deedcoin"	Работает
4.	Контроль за потоками сырьевых материалов в условиях реального производства (стартап "Blockapps")	Компания "BHP Billiton" и компания "ConsenSys"	Работает
5.	Введение защищаемой цифровой документации от несанкционированного доступа	Компания "Maersk" и IBM (США)	Проект
6.	Технологии страховой защиты морских грузоперевозок	Стартап "GuardTime" и компания "Maersk" (США)	Проект
7.	Обмен, хранение медицинских данных и записей	Стартап "Ontology"	Проект
8.	Контроль за цепями поставки морепродуктов	INTEL	Работает
9.	Идентификация музыкального контента	Open Music Initiative (OMI)	Работает в тестовом режиме
10.	Технологии противодействию подделкам продуктов питания «Food Trust Framework»	Alibaba Group, AustPost, PwC	Работает
11.	Контроль и оптимизация учета показателей пробега автомобилей	Корпорация Bosch	Работает
12.	Технологии защиты любых списков, регистрации избирателей, подсчета голосов на выборах	-	Проект
13.	Стартап-индустрия, как источник инвестиций в технологии завтрашнего дня	Компания "Pitch Ventures" (США)	Проект
14.	Децентрализация кодирования медиainформации, ее хранение, распространение	Стартап "Videocoin" (США)	
15.	Технологии "3D- интернет" в образовании и глобальные аудитории для постижения самых современных знаний.	Стартап "SocratesCoin" (США)	Проект

На самом деле отраслей для прорыва в области блокчейн-технологий значительно больше. Предполагаемые области применения блокчейн-технологий, где операндами могут стать не отдельные лица, а коллективы людей, заинтересованных в:

- технологиях рационального распределения товарных ресурсов, прежде всего пищевых продуктов на планете;
- контроле за распространением заболеваний, пандемий, новых видов болезней;
- контроле за распространением по планете некоторых видов млекопитающих, насекомых, вредителей.

Их список с каждым днем расширяется. Например, как следует из отчета банка Credit Suisse для пользователей платежными инструментами типа Visa, Mastercard, WorldPay "технология блочных цепей не представляет большого риска" [1]. Но так ли это?

**Цели работы:** Оценка объективных и необоснованных рисков, связанных с распространением блокчейн-технологий, их возможностей и опасностей как инструментарий для их использования в различных компаниях.

**Результаты исследования.** Так ли уж универсальна эта компьютерная технология? Можно ли сомневаться в ее основных качествах: универсальности для материальных потоков и объективности ухода при этом от посредника (самого главного достоинства блокчейна)? Оценить это можно только практикой, причем эта практика уже в ближайшем будущем даст нам существенную пищу для анализа. Представим некоторые, наиболее часто встречающиеся риски, связанные с использованием рассматриваемых технологий (табл. 2).

Таблица 2.

Риски по источникам возникновения, связанные с использованием блокчейн-технологий в известных областях человеческой деятельности

№№	Наименование риска	Характеристика риска
<i>От производителя блокчейн-технологий</i>		
1	Несопоставимость технических возможностей для пользователей	Ограничения в виде пропускных способностей генерирующих систем для пользователя. Низкая скорость работы из-за криптографии.
2	Появление отдельного сегмента неконтролируемой торговли	Потеря полного контроля со стороны Закона за торговлей, например, запрещенным товаром.
3*	Отсутствие правового поля	Вызывает сомнение в коммерциализации блокчейн-продукции и уход от известных правил ведения бизнеса.
4*	Правило "Атака 50%+"	Риски для ограниченных групп пользователей. Способность обойти партнеров по схеме "подставных фигур".
5*	Отсутствие наработанных организационных методик и единых правил применения	Огромное количество неотработанных и ошибочных технологий, применяемых в отраслях.
6	Неустойчивость к программным взломам блокчейн	До настоящего времени отсутствуют эффективные способы защиты от хакеров.
7	Вмешательство в энергетический ресурс общества	Несопоставимость энергозатрат и реальной стоимости блокчейн-продукта (?)
<i>От потребителя блокчейн-технологий</i>		
8	Распространение нелегального контента, неправомерной информации	Угроза всем участникам сети из-за репликации инородных файлов как заслуживающих доверие.
9	Скрытое отсутствие анонимности	Прозрачность финансов в блокчейн-операциях - прямая опасность для компаний.
10	Безосновательный уход от посредничества в областях, где оно актуально.	1. Движения финансов в компаниях; 2. Криминал, отмывание денег; 3. Некоторые виды торговли.
11*	Недостаточность критического понимания сути блокчейн-технологий	Восприятие большинством пользователей технологий блокчейн как объекта типа "черный ящик" и связанные с этим нарушения и ошибки
12*	Способности к вмешательству в отдельные монополии	Участие бизнеса в неконтролируемых ими операциях в пределе ведет к его разрушению.
13*	Риск криминальных акций	Отмывание обезличенных денег и др.

\* - общепринятые риски

В литературе можно найти и другие риски, с которыми сталкивались пользователи. Рассмотрим некоторые из них.

Первым аргументом против кажущейся универсальности является пресловутое правило "Атака 50%+", когда более половины участников группы задается целью исказить

майнинговые данные. Теоретически это возможно, практически - весьма спорно при достаточно большом количестве игроков в группе. Главный аргумент: меньшинство не сможет обмануть большинство. Например, при нынешнем состоянии майнинга биткойнов такой сговор практически невозможен, так как пользователей этой системы миллионы. Но это относится к вариантам организации массовых финансовых потоков. А как быть с конкретными логистическими операциями, в которых принимает участие ограниченное количество участников? Контроль более половины всех майнингов дает возможность инкогнито переписать всю историю транзакций в виде удобной ее версии и пользоваться своими ресурсами несколько раз. Правило защиты от "Атаки 50%+" может быть преодолено весьма просто. С целью нарушения работы предприятия-конкурента, или с целью увода части материального потока из-под контроля блокчейна, например, при помощи подставных участников, осуществляющих кольцевой обмен. Нет надобности представлять здесь такие схемы. Нужно понимать, что в материальных транзакциях они могут иметь право на существование и ради защиты против них следует уже сейчас искать противоядие. Получается, что выгодность майнинга является залогом успеха в безопасности блокчейн-операций, но чем меньше майнеров, тем система становится более опасной. В особенности, в нефинансовых применениях.

Число доверителей в блокчейн-операциях представляется весьма важным рисковым критерием. Если по этим операциям работают миллионы пользователей - результат понятен. Правило 50+1 не работает. Если потребителей немного, как в любой системе взаимного обмена, то пользователи будут стремиться к расширению числа партнеров. Это один из скрытых механизмов для таких процессов, как создание огромных корпораций их некогда разобщенных фирм, это путь к монополизму на рынке со стороны этих корпоративных объединений. Этот риск сегодня еще не очевиден, но логика такова, что с ним придется справляться в будущем. Блокчейн-технологии вне сферы финансов пока не дают решения этой проблемы. Кстати, компании, владеющие блокчейн-технологиями, уже сегодня ориентируются на свои способности к разрушению некоторых монополий на биржевых рынках посредством вовлечения в неконтролируемую ими децентрализацию. Под такой удар недавно попала компания National Securities Clearing Corporation (NSCC), которой удалось защитить свои интересы, но сам факт уязвимости этого бизнеса от блокчейн-компаний ставит проблемы соответствующих рисков перед ними.

Блокчейны - это всегда риск очутиться вне правового поля. По крайней мере, сегодня это выглядит именно так. Но подвижки в этом вопросе - это вопрос времени. Уже в 2018 году 22 страны Евросоюза подписали соглашение о создании Европейского партнерства в сфере блокчейн-технологий для повышения эффективности вызывающих доверие и ориентированных на пользователя цифровых услуг [2]. По данным агентства Прайм, европейские специалисты подготовят запуск единых для Евросоюза приложений с использованием технологии распределенных реестров для государственного и частного секторов. Пытаясь заполнить нишу, международная организация по стандартизации (ISO — International Organization of Standardization) решила, что международный технический комитет по вопросам разработки стандартов для технологии блокчейн (ISO/TC307) [3] создаст систему стандартов для содействия функциональной совместимости технологий блокчейн, в том числе, ради повышения безопасности и снижения существующих рисков в этих технологиях.

Обсуждаемые проблемы с правовым статусом блокчейн-операций связаны, например, с операциями типа **краудфандинг** - децентрализованное обновление финансовых ресурсов, в частности, в моделях одноранговых накоплений средств вне систем централизованного обслуживания. Например, при помощи платформ типа Kickstarter, Indiegogo или Swarm - краудфандинговой платформы, используемой для накопления средств для стартапов в области цифровых валют. Существование вне правового поля таких действий, когда в них задействованы многие частные компании,

например, с участием в долевом капитале, не может быть полностью легальным, потому что нарушает законодательство о ценных бумагах. Риски в краудфандинговых операциях достаточно велики. Уже сегодня они привели к судебным разбирательствам в компаниях, которые не хотят делиться доходом с обладателями таких децентрализованных платформ, как Manna, Swarmops, DPP и др.

Следующая проблема рисков может иметь место в некоторых случаях безосновательного ухода от посредничества – фактора, который считается главным функциональным достоинством блокчейн-технологий. Да, в тех случаях, о которых чаще всего упоминается в литературе – финансовые операции, работа через банки, такой подход может быть обоснованным. Но если мы говорим о том, что блокчейн-операции претендуют на универсальность как технологии будущего, к такому их качеству следует присмотреться внимательнее.

Контроль следует рассматривать как систему обратной связи в управлении. Классическая система управления подразумевает существование в ней обратной связи: положительной или отрицательной, препятствующей разрушению системы под действием входящих сигналов. Одной из форм существования таких систем является подсистема контроля. В обществе это может быть государственный контроль, общественные формы контроля и др.

Стоит задаться вопросом: так ли уж плоха контролируемость в обществе? По большому счету, уход от контроля, в пределе, может изменить всю государственную систему: могут перестать действовать законы, отпадут за ненужностью контролирующие организации. Уйдет в небытие обратная связь в системах управления как аксиома управления. Стоило бы роль посредника рассматривать и как одну из компонент, обеспечивающих обратную связь. Неконтролируемая торговля – это когда осуществляются логистические цепочки без посреднического контроля. Можно потерять контроль за торговлей наркотиками, людьми, фальшивой валютой и т. д.

Следующим узким местом в любых блокчейн-операциях, в особенности, если число пользователей зашкаливает (что естественно), является несопоставимость объемов скачиваемой информации и мощностей большинства персональных компьютеров. От этого зависит доступ к сети, оперативность получения скачиваемой информации, ее проверка, осуществление платежей или других транзакций. Вариант использования одного центра как альтернатива хранению сразу же противоречит одноранговости в идеологии блокчейна – отсутствие единого посредника. Это риски, с которыми большинство пользователей справляются, например, за счет простых *online*-кошельков, временно (надеюсь) уходя от технологий блокчейна и по-прежнему доверяя серверам. Пропускная способность сети биткойна может составить не более 7 транзакций в секунду. Для примера, скорость обработки у банковской системы Visa – несколько тысяч подобных операций в секунду. Скорость записи транзакций в системе биткойнов составляет не более 0,0166 в секунду. При этом после появления соответствующей записи время ожидания увеличивается в пять раз, так как каждый раз системно считываются все записи без исключения. Таким образом, риск технических возможностей сегодня превышает актуальность ухода в децентрализацию транзакций перед риском иметь посредника. Но это – пока.

Еще один риск связан с уже сейчас появляющимися прототипами программ-взломщиков алгоритмов типа блокчейн. Да, такой вирус будет распознан пользователями этих баз данных и будет распознан. Но она может вмешаться в базы данных, повредить их и сделать непригодными для использования.

Можно надеяться, что блокчейн-технологии получат достаточный уровень безопасности, при их применении в так называемых квантовых компьютерных системах, данные которого по принадлежности к квантовым способам хранения квантовых битов (кубитов) не имеют право сохраняться при искусственном их вскрытии, например. [4]

Но их пока нет и появление их еще долго не предвидится. Хакерские взломы таких программных продуктов могут стать существенным препятствием для их массового применения в самых различных областях. По мнению руководителя отдела блокчейн-технологий Bank of New York Mellon А. Батлина, сегодня еще не существует решений, отвечающих за защиту от взлома с гарантиями для конфиденциальности правовых документов, публичной информации, разрешения споров и транзакций в системе блокчейна [5].

По мнению немецких специалистов, технологии блокчейн уже используются для распространения незаконных, вредоносных данных и нелегального контента [6]. Об этом свидетельствуют и данные Интерпола. При этом хакеров привлекает именно главное свойство технологии - неизменность и неистребимость хэша как носителя этого контента.

Одним из результатов научной конференции "Financial Cryptography and Data Security" стало сообщение немецких ученых из Аахена о выявленных ими 1600 "чужих" добавленных файлов в содержимом в блокчейне, в том числе, детскую порнографию. Там же утверждается, что "помимо распространения нелегального контента, блокчейн также может использоваться для распространения инородного программного обеспечения".

Вне всякого сомнения, не до конца оценен и риск необоснованного вмешательства блокчейн-операций в энергетический ресурс общества. На первый взгляд, затраты электроэнергии на майнинговые действия при помощи компьютеров высокой мощности несопоставимы со стоимостью самого биткойна. Но это только на волне ажиотажа. Если принять во внимание возможную системность такой работы, энергетические затраты на нее могут стать сопоставимыми с энергозатратами крупных металлургических предприятий в год. Энергетические затраты здесь появляются как расплата за децентрализацию, как следствие массовости системных пользователей. Как свидетельствуют эксперты, скорость транзакций при этом не уменьшается.

Существует и широко обсуждаемый риск криминальных акций при использовании блокчейн-технологий. Прежде всего, это возможность обезличенного и бесконтрольного вкладывания денег в криптовалюту с целью их "отмывания". Здесь поле деятельности огромное, и не существует механизмов их контроля по причине отсутствия посредника или контролера. Не всегда следует убирать контроль. Но это проблема правовая и с ней все равно следует считаться и изучать.

Декларируемая анонимность в блокчейн-операциях тоже далеко не всегда является реальностью. Скрытое отсутствие анонимности без присутствия посредника, когда донор транзитирует средства в системе блокчейна, а рецептор их получает, и последний, по крайней мере, оповещается об объеме ресурсов донора и, главное, может видеть историю его транзакций. Согласимся, что это уже не анонимность. Для компаний, участников блокчейн-операций открытость финансов, прозрачность покупок-продаж, финансовая характеристика клиентов, количественные данные счетов, чем сразу воспользуются конкуренты, в определенных условиях, могут привести к банкротству.

Можно оценить реальность указываемых рисков при помощи экспертных оценок, которые дают две группы специалистов из числа разработчиков платформ блокчейн применительно к различным областям, и потребители этих платформ из числа представителей бизнеса, банковской сферы. Всего в исследованиях участвовало 68 человек, которые по 10-бальной шкале дали оценку реальности рисков, указанных в табл. 2. На рис. 1 представлены результаты подобной экспертной оценки.

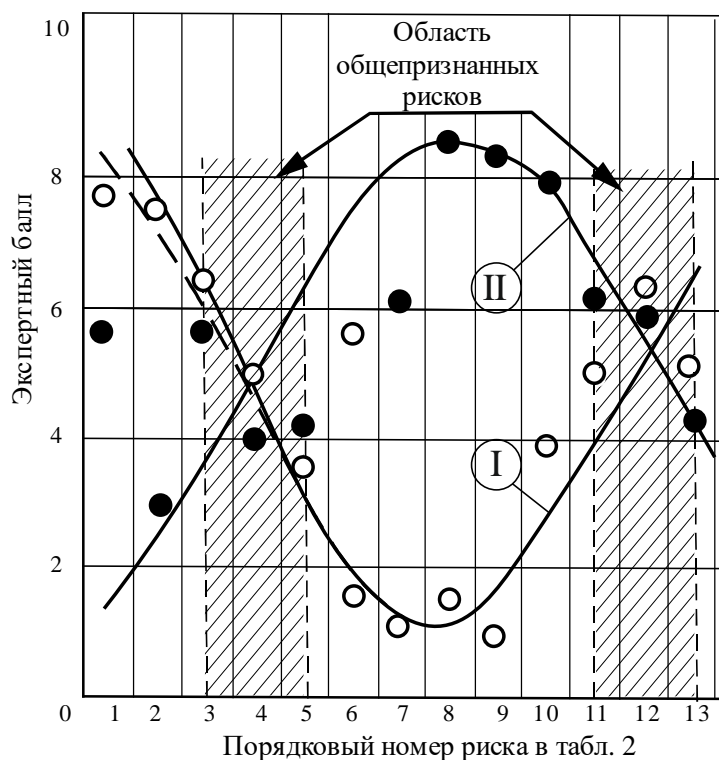


Рис. 1. Экспертная оценка значимости риска по указанным в табл. 2 номерам

В большинстве случаев экспертные оценки представителей двух указанных групп существенно разнятся. Это так называемый парад интересов, который всегда присутствует при продвижении нового товарного продукта. Тем не менее, по ряду позиций (в табл. 2 они обозначены звездочками) оценка рисков, данная производителями и потребителями, практически сходна. Это относится с проблемами правового обеспечения блокчейн-процедур, опасности т. н. "Атаки 50%+", опыта, рациональности и критичности при применении технологий блокчейн в различных областях бизнеса и др. Кроме того, существуют риски криминальные и риски активного вмешательства в конфиденциальные дела компаний.

**Вывод.** Автор имеет возможность утверждать, что существующие реальные и потенциальные риски в известных технологиях блокчейна - это не приговор, но возможность в будущем найти решение этих проблем, предупредить их влияние на инновационные процессы в обществе, обеспечить безопасность человека в нашем стремительно меняющемся мире.

#### Список использованных источников:

1. Блокчейн [Электронный ресурс] = Blockchain: обзор // TAdviser. Государство. Бизнес. ИТ: деловой портал. – Режим доступа: [http://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%91%D0%BB%D0%BE%D0%BA%D1%87%D0%B5%D0%B9%D0%BD\\_\(Blockchain\)](http://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%91%D0%BB%D0%BE%D0%BA%D1%87%D0%B5%D0%B9%D0%BD_(Blockchain))
2. В Австралии разработают стандарты для блокчейна [Электронный ресурс] // Инвест-Форсайт. – 2017. – 16 марта. – Режим доступа: <https://www.if24.ru/v-avstralii-razrabotayut>
3. Евросоюз создал партнерство для развития блокчейн [Электронный ресурс]. – Режим доступа: <https://www.plusworld.ru/daily/tehnologii/evrosoyuz-sozdal-partnerstvo-dlya-razvitiya-blokchejn>
4. Валиев, К. А. Квантовая информатика: компьютеры, связь и криптография / К. А. Валиев // Вестник РАН. – 2000. – Т. 70, № 8. – С. 688–695.
5. Блокчейн может использоваться для распространения нелегального контента [Электронный ресурс]. – Режим доступа: <https://www.securitylab.ru/news/492202.php>

#### References:

1. "Blockchain", ["Blokchejn"], [electronic resource], Blockchain: overview TAdviser. The state. Business. I, business portal, available at:



[http://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%91%D0%BB%D0%BE%D0%BA%D1%87%D0%B5%D0%B9%D0%BD\\_\(Blockchain\)](http://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%91%D0%BB%D0%BE%D0%BA%D1%87%D0%B5%D0%B9%D0%BD_(Blockchain))

2. "In Australia, will develop standards for the Blockchain", ["V Avstralii razrabotajut standarty dlja blokhejna"], [electronic resource], Invest-Forsythe – 2017, 16 March, available at: <https://www.if24.ru/v-avstralii-razrabotajut>
3. "The European Union has created a partnership for the development of the Blockchain", ["Evrosojuz sozdal partnerstvo dlja razvitija blokhejn"], [electronic resource], available at: <https://www.plusworld.ru/daily/tehnologii/evrosoyuz-sozdal-partnerstvo-dlya-razvitiya-blokhejn>
4. Valiev, K. A. (2000), "Quantum Informatics: Computers, Communication and Cryptography", ["Kvantovaja informatika: komp'jutery, svjaz' i kriptografija"], K. A. Valiev, Bulletin of the Russian Academy of Sciences, T. 70, No. 8, pp. 688-695.
5. "The Blockchain be used to distribute illegal content", ["Blokhejn mozhet ispol'zovat'sja dlja rasprostraneniya nelegal'nogo kontenta"], [electronic resource], available at: <https://www.securitylab.ru/news/492202.php>

**Keywords:** blockchain; crowdfunding; blockchain technology; innovation processes.

**Ключові слова:** блокчейн; краудфандинг; блокчейн-технології; інноваційні процеси.

**Ключевые слова:** блокчейн; краудфандинг; блокчейн-технологии; инновационные процессы.

Рецензент: М. Г. Белопольський, завідувач кафедри обліку і аудиту ДВНЗ «Приазовський державний технічний університет», віце-президент Академії економічних наук України, голова спеціалізованої вченої ради Д 12.052.02, д. е. н., професор

Перевірено на плагіат системою: <https://corp.unicheck.com/library/viewer/report/5015913>