СТРАТЕГИЯ ПОВЫШЕНИЯ ФИНАНСОВОЙ ГРАМОТНОСТИ
В РОССИЙСКОЙ ФЕДЕРАЦИИ НА 2017-2023 ГОДЫ

ФИНАНСОВОЕ КОНСУЛЬТИРОВАНИЕ

МИНИСТЕРСТВО ФИНАНСОВ
Российской Федерации

ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Риски криптовалют

Как устроена система Blockchain.

Дословно blockchain переводится как цепочка из связанных друг с другом блоков. В таких «ячейках» содержится информация, зашифрованная в цифровом виде.

Блокчейн — это неизменяемая распределенная база данных для одноранговых транзакций.

«Неизменяемая» означает, что информация, внесённая в такую базу данных, не может быть отредактирована или удалена.

«Распределённая» — это значит, что база физически не хранится на одном компьютере или сервере, а распределена по разным компьютерам.

База данных — информация, упорядоченная по определённым критериям. В нашем случае речь идёт о хранении данных в электронном виде.

Одноранговые транзакции — это логически осмысленная операция, совершённая между участниками сети напрямую, без участия третьей стороны. Это понятие наиболее распространено в финансах, и в качестве примера можно привести P2P-торговлю.

База данных состоит из блоков, где и хранится история транзакций. Новый блок всегда привязан к предыдущему и имеет ссылку на него. Большое количество связанных между собой блоков образует экосистему, которую практически невозможно взломать.

Отсюда и **название Blockchain** — «цепочка из блоков», где каждый блок — это фрагмент информации обо всех транзакциях, контрактах или сделках, проводимых в сети между её участниками.

Bitcoin и blockchain можно назвать взаимозаменяемыми, но между ними есть разница. Основа биткойна — это та самая технология блокчейн. Многие по ошибке используют эти понятия как равнозначные, однако blockchain применяется не только в сфере криптовалют.

Bitcoin представляет собой централизованную валюту, которая изначально создавалась для проведения интернет-транзакций. Сегодня она имеет статус цифрового актива, который можно перевести в реальные деньги. Биткойн-блокчейн, находящийся в публичном доступе, создает и управляет централизованным реестром. Его копии хранятся на многочисленных серверах, размещенных по всему миру.

Риски Blockchain.

Технология распределенного реестра известна своей безопасностью. Однако это не означает, что она полностью защищена. В самой системе блокчейн существует достаточное количество рисков.

1) Риски, связанные с человеческим фактором.

Хотя блокчейн полностью децентрализован, он все равно должен взаимодействовать с людьми, чтобы работать правильно. В этом случае возникают новые угрозы безопасности для блокчейна. Например, любой бизнес, который хочет взаимодействовать с системой блокчейна, должен делать это либо через компьютер, либо через автоматизированные системы. Когда пользователь взаимодействует через компьютер, в этот момент существует вероятность того, что учетные данные для доступа к системам могут быть украдены или взломаны. Это происходит только в конечных точках, что делает блокчейн уязвимым.

2) Риски, связанные с частным и публичным ключами.

Вся идея технологии блокчейна в значительной степени опирается на частный и публичный ключи. Эти ключи представляют собой серию символов, которые предлагают уникальные свойства безопасности. Одним из свойств безопасности является то, что это трудно угадать.

Блокчейн работает с этими ключами. Если у вас нет правильной комбинации частного или публичного ключа, вы просто не сможете получить доступ к цифровому контенту, хранящемуся в блокчейне. Хакеры знают это, и они также знают, что угадывать эти ключи — пустая трата времени. Вот почему они пытаются получить ключи, атакуя самое слабое место, то есть систему, которую использует пользователь. Это может быть мобильное устройство или персональный компьютер.

3) Риски, связанные с поставщиками.

Многие специальные платформы и сервисы работают с технологией распределенного реестра для улучшения его функциональности. К этому относятся такие решения, как кошельки, платежные системы, смарт-контракты, платежные платформы блокчейна и т. д. Эти поставщики также представляют риск для пользователей. Если используемая платформа или служба имеют какую-либо форму уязвимости, то при доступе к ней могут возникнуть проблемы.

4) Непроверенный код.

Качество кода остается большой проблемой для большинства решений блокчейна. Таким образом, угроза безопасности может возникнуть из-за плохого кода, слабой системы безопасности и неправильного использования со стороны людей. Кроме того, так как большинство поставщиков программ используют смарт-контракты, они должны гарантировать, что их смарт-контракты свободны от всевозможных недостатков или лазеек в безопасности. Если имеется хотя бы один, это может легко привести к общесистемному эффекту.

Риски Криптовалют.

Прежде всего, нужно понимать, что при проведении операций с криптовалютой не происходит ее фактический обмен, а проводится смена владельца записи (цифровой монеты).

Криптовалютный кошелек — ПО для взаимодействия с Реестром. Существует два вида криптовалютных кошельков — **горячие и холодные**.

Выбор бумажника для криптовалюты напрямую зависит от суммы, которую предполагается хранить на счету. Если необходимо часто проводить транзакции, то для этого лучше сразу выбирать горячие кошельки. Холодные не могут похвастаться удобством при постоянном использовании, они больше подойдут для длительного хранения основной части капитала.

Горячий кошелёк — это, по сути, программа, которая может подключаться к различным блокчейнам. Представляет собой браузерное расширение (для компьютера) или мобильное приложение (для телефона). Важно понять, что непосредственно в браузере или на вашем

компьютере монеты не хранятся, они там всего лишь отображаются, сами монеты находятся в сети блокчейна. Их нельзя вывести на какой-то оффлайн кошелёк, чтобы они лежали там отдельно от других монет в этой сети. Просто эти активы числятся за определенным номером кошелька, и это фиксируется в блокчейне .

При регистрации криптокошелька необходимо записать **seed-фразу**. Это как раз ключ, который позволяет получить вам доступ к конкретному кошельку на конкретном блокчейне и управлять средствами.

Холодный кошелек является более безопасным местом хранения своих активов. Он бывает десктопный или же может представлять из себя физический носитель (выглядит это как флешка). Холодный аппаратный кошелек может пригодиться в тех случаях, когда нужно хранить крупные суммы. Его же можно использовать и для безопасного проведения транзакций.

Холодный аппаратный кошелек может пригодиться в тех случаях, когда нужно хранить крупные суммы. Его же можно использовать и для безопасного проведения транзакций. Физический носитель для холодного кошелька не стоит покупать на Авито или Ozon, только напрямую у поставщика. На российских маркетплейсах каждый второй холодный кошелёк перепрошит, и вы рискуете сразу, как его пополните, потерять все свои средства.

В качестве рисков криптовалют однозначно можно обозначить следующее.

1. Никаких гарантий на возмещение ваших убытков. Законодательство не регулирует перемещение ваших средств. Активы принадлежат только бирже и контролируются в ее пределах. Площадкой предоставляется лишь доступ для входа в систему, и владельцу приходится доверить безопасности сервера свой кошелек.

2. Волатильность курса криптовалюты формирует ее нестабильность. Это означает непредсказуемость изменения цены активов. При волатильности во многих источниках появляется различная информация, в том числе и ложная, что может лишь усугубить ситуацию.

3. Риск торговых площадок. В случае банкротства биржи средства потеряют все ее участники. К примеру, исчезновение площадки Einstein принесло пользователям убыток в 16 миллионов долларов. Кроме того, обман клиентов производится и без закрытия биржи. К примеру, путем повышения тарифов вывода денежных средств.

4. Угроза для финансовой стабильности государства. Возможное использование криптовалюты в качестве платежа создает угрозу для национальной валюты. Это может привести к высокому уровню инфляции и ограничить эффект от проведения денежно-кредитной политики. Такие последствия несут угрозу для благосостояния бизнеса и государства.

5. Вредоносное программное обеспечение. Преступники используют его для кражи криптомонет. Число способов мошенничества значительно выросло за последние годы. К распространенным методам обмана пользователей относят:

- вирусы-вымогатели;
- фальшивые ссылки;
- поддельные сайты;
- фишинг.

6. Отсутствие полноценного контроля. Правила инвестирования цифровых денег не закреплены в законодательстве РФ и во многих других странах, поэтому государство не контролирует оборот криптовалюты. Тем не менее данная сфера притягивает преступников, поэтому правительство все чаще проводит дискуссии по поводу организации механизмов оборота цифровых активов.

Если средства были украдены с криптокошелька, у его владельца нет шансов определить вора и подтвердить право на монеты. Страховых гарантий также не предусмотрено, поэтому инвесторы надеются только на себя и на выбранные биржи.

7. Потеря секретного кода.

Код является вашим доступом к криптовалютному кошельку. Его потеря подразумевает утрату всех ваших активов. Восстановление кода невозможно, поэтому необходимо хранить и беречь свои данные. Суммы

потерь по причине сбоя флеш-носителей, на которых записан код, составляет уже десятки миллиардов долларов.

Основные различия между электронными деньгами и криптовалютой.

Криптовалюты изначально позиционировались как инструменты распространения интеллектуальной собственности и финансовой ценности, более совершенный механизм платежей, средство расширения доступа к финансовым услугам и способ устранения финансовых посредников. К текущему моменту цифровые активы не принесли ни одного из этих преимуществ.

Утверждения, что криптовалюты являются эффективным средством сбережения и платежным средством, до сих пор не выдерживают критики. Как деньги, инструмент должен иметь стабильную стоимость и ограниченную волатильность цен, в случае с криптовалютами этого нет.

Аналогичные вопросы поднимаются в отношении **стейблкоинов,** держатели которых могут столкнуться с ситуацией отсутствия «контрагентов для выхода из позиций». Подобные активы пока слишком рискованны, чтобы выступать платежным средством.

Больше перспектив стать одной из форм денег есть у цифровой валюты Центрального банка.

Для более полного понимания различий между формами денег целесообразно сравнить четыре формы: **банкноты, депозитные деньги, электронные деньги и цифровую валюту.**

Как видно из таблицы 1, основным отличием цифровых денег от других безналичных форм денег является то, что цифровая валюта существует не в виде записи на счете владельца на сервере финансовой организации, а в виде цифрового кода. В отличие от электронных денег, цифровая валюта беспрепятственно может быть использована как при доступе в интернет, так и без него.

Таблица 1.

Признак	Наличные	Депозитные (счета в банках)	Электронные (счета в НКО и т. п.)	Цифровые
Форма существования	Бумажные банкноты или монеты	Запись в базе данных коммерческих банков или ЦБ	Запись в базе данных эмитентов – НКО, банки и др.	Цифровой код
Эмитент	ЦБ	Коммерческие банки (распределяются через ЦБ)	НКО и другие в соответствии с нормативами	ЦБ
Персонализация	На предъявителя	Персонализи-рованные	Персонализированные либо на предъявителя	Персонализи-рованные либо на предъявителя
Возможность онлайн использования	Нет	Есть (нельзя без доступа к интернету)	Есть в двух вариантах – через сеть (сетевые ЭД) и через чип без доступа к интернету (смарт-карты)	Есть (можно без доступа к интернету)
Возможность офлайн использования	Есть	Нет	Есть (чипы смарт-карт)	Есть

Риски бесконтактных платежей.

Бесконтактные банковские карты используют для передачи данных технологию NFC, разновидность RFID. На карте размещены чип и антенна, которые «откликаются» на запрос платежного терминала на радиочастоте 13,56 МГц. Разные платежные системы используют собственные стандарты: Visa payWave, MasterCard, PayPass, American Express, ExpressPay и так далее. Но устроены они похожим образом.

Безопасность обеспечена несколькими факторами.

1) Расстояние. Дальность передачи данных через NFC составляет несколько сантиметров. Поэтому первый барьер защиты — физический. Считыватель, по сути, необходимо приложить вплотную к карте, что довольно сложно сделать незаметно.

2) Криптография. Приблизиться к карточке — это один вопрос. Дальше нужно преодолеть более серьезную защиту, основанную на криптографии.

Бесконтактные транзакции защищены тем же стандартом EMV, что и чиповые карты. По запросу терминала микросхема каждый раз генерирует одноразовый ключ. Этот ключ можно перехватить, но он уже не подойдет для следующей транзакции.

В стандартной реализации защита чиповых карт строится на комбинации криптоключей и ввода пользователем PIN-кода. При

бесконтактных транзакциях PIN-код обычно не запрашивается, так что остаются только криптоключи чипа карты и терминала.

Сделать терминал, который будет считывать данные карты из кармана клиента, теоретически возможно. Но этот терминал должен иметь установленные криптографические ключи, полученные у банка-эквайера и платежной системы. Ключи выдаются по договору с юридическим лицом, то есть с банком-эквайером. Таким образом, мошенничество будет легко обнаружить.

3) Сумма покупки. Есть еще один уровень защиты — ограничение максимальной суммы бесконтактной транзакции. Этот предел в настройках терминального оборудования задает банк-эквайер, руководствуясь рекомендациями платежных систем. В России максимальный порог платежа составляет 1000 рублей, в США — $25 и т.д.

Технология бесконтактных платежей действительно закрыта хорошей многофакторной защитой. Тем не менее многое зависит от добросовестности настроек конкретных финансовых учреждений и магазинов. Причем последние в погоне за высокой скоростью покупок и низким процентом «брошенных корзин» нередко очень сильно пренебрегают безопасностью платежа.

МИНИСТЕРСТВО ФИНАНСОВ
Российской Федерации

ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ