**«Уникальность рисков, связанных со смарт-контрактами и технологией блокчейна»**

***Касси Дафиссу Одри\* (МГРИ,*** [***kassidafissouaudrey@gmail.com***](mailto:kassidafissouaudrey@gmail.com)***),***

***Шийко В.Г. (МГРИ,*** [***shiikovg@mgri.ru***](mailto:shiikovg@mgri.ru))

Аннотация

В этой статье освещается уникальность рисков, связанных со смарт-контрактами и технологией блокчейн. В век просвещения, когда новые технологии переживают бум, смарт-контракты становятся инновационной формой договорных отношений во всех сферах деятельности. Однако эти цифровые «гении» не лишены рисков. В этой статье рассматриваются возможные риски, связанные с использованием смарт-контрактов и приводятся некоторые рекомендации по их решению.

Ключевые слова

Смарт-контракт, блокчейн-проект, цифровые технологии, риски, инновационные подходы, кибератаки.

Теория

Технологии блокчейна и смарт-контрактов с уверенностью можно отнести к революционным способам осуществления сделок и заключения договоров. Вместе с тем, данные инновационные подходы сопряжены с определенными рисками, которые необходимо выявлять и контролировать.

Риски, связанные со смарт-контрактами и технологией блокчейна, разнообразны и многолики. Среди них различают следующие виды.

**Технические и операционные риски**

Смарт-контракты - это программы, которые автоматически выполняются при соблюдении заранее заданных условий. Реализация и программирование смарт-контрактов требует специальных технических знаний, что может привести к ошибкам и уязвимостям. Кроме того, после записи смарт-контракта в блокчейн он не может быть изменен, что создает проблемы в случае возникновения ошибок или необходимости внесения изменений. Кроме того, в смарт-контрактах возможны ошибки. Поскольку смарт-контракты являются самоисполняющимися, и условия контракта записываются непосредственно в код, ошибки в котором могут привести к непредвиденным последствиям, в том числе к потере финансовых средств.

**Безопасность и конфиденциальность**

Блокчейн использует передовые технологии шифрования для защиты данных, а смарт-контракты хранят конфиденциальную информацию, которая может быть уязвима для кибератак. Полная прозрачность, которую обеспечивают блокчейны, снижает риск мошенничества и злоупотреблений, но отсутствие посредников создает необходимость повышенной бдительности в отношении кибератак.

**Правовые и нормативные проблемы**

Поскольку блокчейн - относительно новая технология, нормативно-правовая база все еще остается неопределенной и развивающейся. Изменения в нормативно-правовой базе могут повлиять на жизнеспособность блокчейн-проектов.

Отсутствие ясности в нормативно-правовой базе может препятствовать использованию смарт-контрактов в некоторых отраслях.

Организациям необходимо ознакомиться с местными и международными нормативными актами, касающимися использования блокчейна.

**Сложность внедрения**

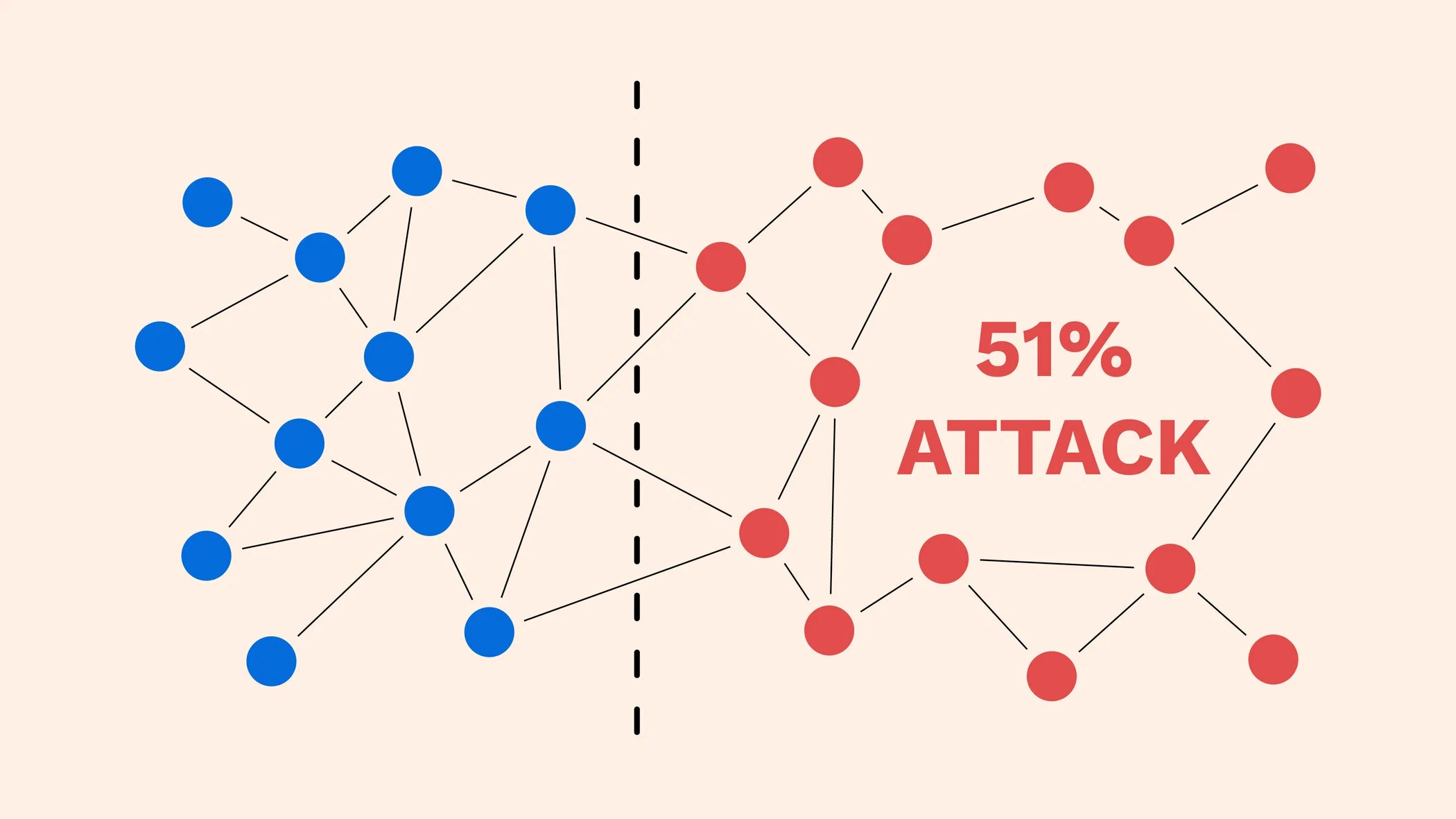
Внедрение блокчейна - это сложный процесс, требующий соответствующей инфраструктуры и обучения персонала.

Взаимодействие между различными платформами блокчейна остается серьезной проблемой. Различные сети блокчейна могут быть несовместимы друг с другом, что может привести к проблемам со связью и передачей данных между ними.

**ИТ-безопасность**

Кибератаки, такие как атаки 51%, атаки Sybil и атаки грубой силы, могут ослабить безопасность блокчейна.

Атака 51 % происходит, когда злоумышленник контролирует более 50 % вычислительных мощностей блокчейна. Это дает злоумышленнику контроль над большинством блоков, добавленных в блокчейн, что позволяет ему манипулировать транзакциями. На рисунке 1 графически изображено действие атаки 51%, где Майнинг-пул MineXMR угрожает блокчейну Monero атакой 51%.



***Рисунок 1.*** *Действие атаки 51 %.* *Майнинг-пул MineXMR угрожает блокчейну Monero атакой 51%.*

**Атаки сибилов**

Атаки Sybil происходят, когда злоумышленник формирует несколько идентификаторов (узлов) в децентрализованной сети, создавая впечатление, что мощности распределены более широко, чем на самом деле. Это может нарушить консенсус и безопасность блокчейна.

**Атаки грубой силы**

Атаки грубой силы подразумевают попытку получить доступ к учетной записи путем перебора множества возможных комбинаций закрытых ключей, пока не будет найдена правильная комбинация. Если закрытые ключи недостаточно надежны, этот метод может нарушить безопасность учетной записи.

Чтобы уменьшить эти риски, необходимо внедрить надежные механизмы безопасности, такие как устойчивые хэш-алгоритмы (хэш-алгоритм - это математическая функция, которая шифрует данные так, чтобы их невозможно было прочитать; эти алгоритмы являются односторонними программами, которые не позволяют другим расшифровать текст), безопасные протоколы консенсуса и конфиденциальные инструкции управления ключами.

Другими важными аспектами управления безопасностью блокчейна являются внедрение надлежащих практик безопасности, постоянный мониторинг сети и активное участие участников в выявлении и уменьшении потенциальных угроз.

Риски, связанные со смарт-контрактами и технологией блокчейна, могут быть снижены с помощью различных решений.

Для снижения рисков важно активно содействовать повышению осведомленности, просвещению и демонстрации практических преимуществ блокчейна. Сотрудничество между заинтересованными сторонами, усилия по стандартизации и прозрачная передача успешных примеров использования могут способствовать более широкому и устойчивому внедрению технологии блокчейна.

**Углубленный аудит и тестирование**

Тщательный аудит смарт-контрактов необходим для выявления и устранения потенциальных уязвимостей. Тщательное тестирование помогает обеспечить надежность и безопасность смарт-контрактов.

**Использование стандартов и передовой практики**

Использование стандартов проектирования и лучших практик безопасности при программировании смарт-контрактов позволяет снизить риск ошибок и нарушений безопасности.

**Страхование и управление рисками**

Страхование смарт-контрактов может быть рассмотрено для покрытия убытков, которые могут возникнуть в случае неудачи контракта. Также следует активно управлять рисками, связанными с блокчейном и смарт-контрактами.

**Управление и механизмы возмещения ущерба**

Создание механизмов управления, которые могут быть изменены или дополнены по мере необходимости, поможет снизить риски, связанные с неизменяемостью смарт-контрактов.

**Образование и осведомленность**

Обучение разработчиков и пользователей надлежащим методам обеспечения безопасности, связанным со смарт-контрактами и блокчейном, необходимо для снижения операционных рисков.

**Нормативно-правовая база**

Четкая нормативно-правовая база, связанная со смарт-контрактами, может помочь снизить юридические риски и повысить доверие к использованию этой технологии.

Важно отметить, что эти решения не гарантируют полного устранения рисков, но они могут помочь минимизировать уязвимости и повысить надежность и безопасность смарт-контрактов и технологии блокчейн.

**Выводы**

Смарт-контракты и технология блокчейна дают значительные преимущества с точки зрения результативности и снижения затрат при оформлении и исполнении договорных отношений. Для максимального раскрытия и использования потенциала этих инновационных технологий необходимо эффективное выявление и управление возможными рисками. Полная безопасность активов и транзакций особенно ценна в отраслях, где очень важны качество, высокая производительность (большое количество транзакций в секунду), низкое потребление электроэнергии, безотзывность сделок и высокая устойчивость к кибератакам.

Библиография

1. Аналитический обзор по теме «Смарт-контракты» // Центральный банк Российской Федерации: [официальный сайт]. – 2018. – URL: https://cbr.ru/Content/Document/File/47862/SmartKontrakt\_18-10.pdf.
2. Булгаков И. «Умные» контракты и современное договорное право // Zakon.ru: [сайт]. – 2016. – URL: https://zakon.
3. Бурсье Д., Де Филиппи П. «Прозрачность алгоритмов перед лицом открытых данных: в каком состоянии данные»РФАП 2018, № 167, С. 525.
4. Вашкевич А. М. Смарт-контракты: что, зачем и как– Москва: Симплоер,2018.– 89 с.
5. Кембриджский справочник по смарт-контрактам, технологии блокчейн и цифровым платформам, С. 334 – 358.
6. Осмоловская А.С. Смарт-контракты: функции и применение / Осмоловская А.С. // Бизнес-образование вэкономике знаний. – 2018. – №2. – С. 54–56.
7. Поля Х. «Административные решения и алгоритмы: преданность профессии», РДП 2018, С. 641.
8. Szabo N. Smart Contracts: Building Blocks for Digital Free Markets. – 1996. – URL: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart\_contracts\_2.html.

**Bibliography**

1. Analytical review on the topic "Smart contracts" // Central Bank of the Russian Federation: [official website]. – 2018. – URL: https://cbr.ru/Content/Document/File/47862/SmartKontrakt\_18-10.pdf.

2. Bulgakov I. "Smart" contracts and modern contract law // Zakon.ru : [website]. – 2016. – URL: https://zakon.

3. Bourcier D., De Philippi P. "Transparency of algorithms in the face of open data: in what state is the data" RFAP 2018, No. 167, p. 525.

4. Vashkevich A.M. Smart contracts: what, why and how - Moscow: Simpler, 2018.– 89 p.

5. Cambridge Handbook of Smart Contracts, blockchain Technology and Digital Platforms, pp. 334-358.

6. Osmolovskaya A.S. Smart contracts: functions and applications / Osmolovskaya A.S. // Business education in the economics of knowledge. - 2018. – No.2. – pp. 54-56.

7. Fields H. "Administrative solutions and algorithms: dedication to the profession", RDP 2018, p. 641.

8. Szabo N. Smart Contracts: Building Blocks for Digital Free Markets. – 1996. – URL: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart\_contracts\_2.html.