# Сайдчейны, кроссчейн-мосты и вопросы безопасности

**Александр Подобных,** *руководитель Санкт-Петербургского РО АРСИБ, руководитель Комитета по безопасности цифровых активов и противодействию мошенничеству, судебный эксперт*

Сайдчейны и кроссчейны — это красивые инженерные решения для масштабирования и расширения функциональности блокчейнов, они открывают новые возможности для взаимодействия между различными сетями. Однако с собой они приносят и новые риски в части безопасности. По мере роста популярности системы сайдчейнов и кроссчейнов становятся объектами повышенного внимания злоумышленников и вопросы, связанные с целостностью, конфиденциальностью и доступностью данных, становятся для них все более актуальными.

## Сайдчейны

Сайдчейн (Sidechain) – это технология, которая позволяет создавать дополнительные цепи данных, связанные с основной блокчейн-сетью. Идея заключается в том, чтобы улучшить определенные характеристики или функциональность блокчейна, вынося часть операций за пределы базовой цепи. Пользователи могут перемещать свои активы между основной цепью и сайдчейном. Это позволяет улучшать масштабируемость, ускорять транзакции или добавлять новые функции без необходимости внесения изменений в основной блокчейн.

Например, сайдчейн сети Ethereum под названием Polygon PoS обладает производительностью, почти в 500 раз превосходящую скорость родительской сети.

## Кроссчейн-мосты

В отличие от сайдчейнов, которые обычно работают как дополнительные цепи данных внутри одной блокчейн-системы, кроссчейны предполагают взаимодействие между различными блокчейнами, зачастую даже принадлежащими к разным протоколам.

Идея кроссчейна состоит в том, чтобы позволить перемещение активов и данных между разными блокчейнами, обеспечивая интероперабельность между сетями.

## Немного истории

В начале блокчейн-эры, когда появился биткоин, первая и самая известная блокчейн-сеть, стали проявляться ограничения по производительности. Блоки в цепи формировались примерно каждые 10 минут, и существовали ограничения на количество транзакций, которые могли быть включены в один блок.

С увеличением популярности криптовалют и блокчейна стало очевидным, что необходимы решения для улучшения производительности и масштабируемости. Задержки в подтверждении транзакций и ограничения по пропускной способности стали проблемами, требующими решения.

Концепция сайдчейнов начала формироваться как способ решения проблем масштабируемости. Идея заключалась в том, чтобы выносить часть транзакций или операций за пределы основной блокчейн-цепи, чтобы улучшить ее производительность, не изменяя саму цепь.

С течением времени и с развитием блокчейн-технологий исследователи и разработчики начали предлагать конкретные решения и протоколы для реализации сайдчейнов.

Различные проекты начали проводить эксперименты с сайдчейнами, тестируя их в реальных условиях. Это позволило сообществу лучше понять преимущества и ограничения данного подхода.

Важно понимать, что каждый сайдчейн самостоятельно обеспечивает свою безопасность. В случае компрометации ущерб остается в рамках этой цепи и не затрагивает основной блокчейн. С другой стороны, если будет скомпрометирован основной блокчейн, сайдчейн продолжит работать, но его привязка к родительской цепи обесценится.

## Сходства и различия

Обе концепции направлены на улучшение масштабируемости блокчейна. Они предоставляют механизмы для обработки большего количества транзакций и увеличения производительности системы.

Сайдчейны и кроссчейны разгружают основную цепь от избыточных операций, обеспечивая более эффективное использование ресурсов. Используя сайдчейны и кроссчейны, разработчики могут расширить функциональность своих приложений, добавляя новые возможности и операции.

Смарт-контракты являются строительными блоками для создания сложных и безопасных операций как внутри одного блокчейна, так и между различными блокчейнами. Их автоматизированные и программируемые характеристики существенно улучшают функциональность и эффективность сайдчейнов и кроссчейнов.

Смарт-контракты облегчают выполнение транзакций между различными блокчейнами. Они принимают условия и проверки с одной цепочки и инициируют запрограммированные действия на другой.

## Атаки на кроссчейны

### Double-Spending

Атака Double-Spending направленна на многократное использование одних и тех же активов в разных блокчейнах. Double-spending реализуется, когда атакующий отправляет одновременно две или более транзакции, расходуя одни и те же криптовалютные средства. Типичным примером Double-Spending является сценарий Race Attack, при котором атакующий одновременно отправляет две разные транзакции с одинаковыми средствами. Злоумышленник рассчитывает, что обе транзакции будут включены в блоки, что может сработать в блокчейнах с длительным временем генерации блоков.

В малоиспользуемых или низкоуровневых блокчейнах, которые обычно отли-