

# Доказательство с нулевым разглашением и его роль в информационной безопасности

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



Довольно часто фундаментальные исследования прошлого века обретают новую жизнь в современном мире, находя свое применение на переднем крае технологий. Одним из таких примеров стала идея доказательства с нулевым разглашением, которая органично вписалась в вопросы информационной безопасности.

## Что такое доказательство с нулевым разглашением?

Доказательство с нулевым разглашением (Zero-Knowledge Proof, ZK-доказательства, ZKP) – это криптографический протокол, который позволяет одному лицу (доказывающему) убедить другого (проверяющего) в том, что некоторое конкретное утверждение верно, не раскрывая никаких подробностей о самом утверждении. То есть одна сторона может доказать, что знает секретные данные, не раскрывая их или их детали, а вторая может только убедиться, что доказывающая сторона имеет доступ к этой информации.

Эта концепция играет важную роль в информационной безопасности вообще и в сфере блокчейн-технологий в частности. В качестве примеров ее применения можно привести аутентификацию без раскрытия пароля, проверку ПДн без их публикации, доказательство владения определенным частным ключом в блокчейне без публичного раскрытия этого ключа.

## История вопроса

Идея доказательств с нулевым разглашением была предложена в работе "The Knowledge Complexity of Interactive Proof-Systems" авторами Шафи Голдвассер, Сильвио Микали и Чарльз Раккофф в далеком 1985 г.

Исследователи представили новый класс протоколов интерактивных доказательств, которые позволяют одной стороне доказывать свое знание о неко-

торой информации без раскрытия самой информации. Этот важный концепт привлек много внимания и был затем усовершенствован в последующих работах.

Канонически доказательство с нулевым разглашением должно соответствовать следующим трем критериям:

- **полнота:** проверяющий примет доказательство с высокой вероятностью, если утверждение истинно, а проверяющая и доказывающая сторона придерживаются протокола;
- **обоснованность:** если утверждение не соответствует действительности, ни один доказывающий не должен быть в состоянии убедить проверяющего в обратном, за исключением случаев стечения крайне маловероятных обстоятельств;
- **нулевое знание:** даже после взаимодействия с доказывающей стороной проверяющий понимает только истинность утверждения и ничего больше не знает о секрете.

Понятие знания играет фундаментальную роль в концепции доказательств с нулевым разглашением. Знание описывает информацию или данные, которые доказывающая сторона знает или обладает ими. Это может быть, например, секретный ключ, пароль, номер паспорта и т.п.

Доказательство знания заключается в том, чтобы, используя математические и криптографические методы, убедить проверяющую сторону, что доказывающая сторона реально обладает знанием, не раскрывая при этом сами данные или информацию.

Примером реализации идеи может служить неинтерактив-

ный протокол ZK-SNARK (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge). Неинтерактивность в данном случае подразумевает, что доказательство представляет собой блок данных и не требует прямого взаимодействия сторон протокола.

## Роль цифровой подписи в ZK-доказательствах

Цифровая подпись – это важный компонент для создания безопасных и приватных ZK-доказательств, позволяющий доказывающей стороне аутентифицировать себя и подтвердить правильность утверждений без раскрытия конфиденциальных данных. Цифровая подпись позволяет доказать, что отправитель знает закрытый ключ, который соответствует открытому ключу, используемому для верификации.

Подпись также обеспечивает подтверждение целостности данных. В ZK-доказательствах отправитель может использовать цифровую подпись для демонстрации того, что данные не были изменены после их подписания.

Цифровая подпись может использоваться в ZK-доказательствах для подтверждения правильности определенных операций без раскрытия конкретных данных. Например, отправитель может подписать хеш данных и предоставить его для верификации вместо самих данных.

## Области применения

Конечно же, ZK-доказательства для повышения конфиденциальности транзакций и масштабируемости имеют важное значение в мире блокчейна как

Идея доказательств с нулевым разглашением была предложена в работе "The Knowledge Complexity of Interactive Proof-Systems" авторами Шафи Голдвассер, Сильвио Микали и Чарльз Раккофф в далеком 1985 г.