УДК 621.3.049.77–048.24:537.2

КРИПТОГРАФИЧЕСКОЕ ОБОСНОВАНИЕ СТОЙКОСТИ NFT НА БАЗЕ СМАРТ-КОНТРАКТОВ ETHEREUM

Плетинский И.В., студент гр.951007

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Нестеренков С.Н. – канд. техн. наук

Аннотация. Был изучен стандарт ERC 721 для невзаимозаменяемых токенов на базе смарт-контрактов Ethereum и техническая документация. Были изучены используемые криптографические алгоритмы, структуры данных и алгоритмы подтверждения транзакций в блокчейне. Было дано обоснование криптографической стойкости NFT на базе смарт-контрактов Ethereum. Была разработана методика аудита кода смарт-контракта NFT.

Ключевые слова. NFT, ERC 721, смарт-контракт, SHA-256, эллиптические кривые, доказательство доли владения

Невзаимозаменяемый токен (NFT) — вид криптографических токенов, каждый экземпляр которого уникален, не может быть отредактирован или замещен. Токены могут иметь любое содержание, например, текстовые данные или медиаконтент. Они используются для подтверждения авторства, для электронной цифровой подписи, для подтверждения права собственности на цифровые активы в рамках блокчейна.

В данной статье рассматриваются используемые криптографические алгоритмы и алгоритм консенсуса “Доказательство доли владения”, обеспечивающие уникальность, неподделываемость, необратимость и возможность определения владельца NFT.

Стандарт ERC 721 [1] описывает требования к смарт-контрактам Ethereum для удовлетворения критериям невзаимозаменяемых токенов и для развёртывания смарт-контрактов в любых Ethereum сетях.

Потенциальные вектора атак злоумышленников на смарт-контракты невзаимозаменяемых токенов могут быть направлены на [2]:

– подмена содержимого блоков в блокчейне;

– редактирование содержимого токенов;

– непосредственно кража NFT, т.е. изменения владельца.

Для обеспечения криптографической стойкости смарт-контрактов к перечисленным выше атакам используются следующие алгоритмы:

– алгоритм хэширования SHA256;

– алгоритм цифровой подписи на основе эллиптических кривых;

– алгоритм консенсуса “Доказательство доли владения”.

Алгоритм SHA-256 является криптографической хеш-функцией, которая используется для создания уникального идентификатора фиксированной длины из произвольных данных. Алгоритм обеспечивает целостность данных блока в блокчейне. На рисунке 1 изображен принцип использования алгоритма SHA-256 при записи данных в блокчейн:

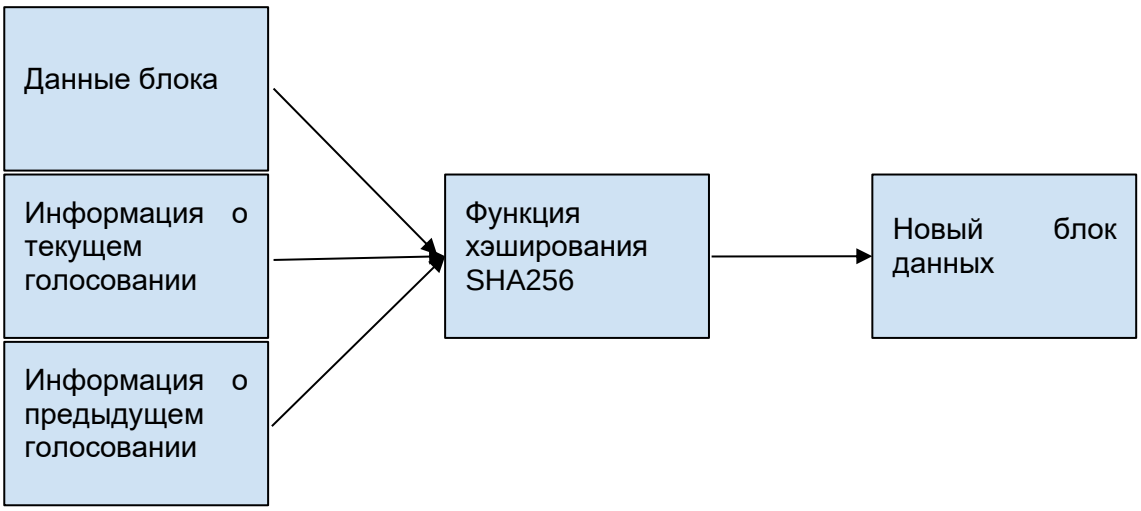

Рисунок 1 – Принцип использования алгоритма SHA-256

Алгоритм цифровой подписи на основе эллиптических кривых (ECDSA) используется для подписи транзакций и обеспечения их целостности. Он основывается на математической теории эллиптических кривых и использует дискретный логарифм для создания ключей и подписей. Для генерации ключей используется приватный ключ, который является случайным числом, и публичный ключ, который является точкой на эллиптической кривой. Эллиптическая кривая в ECDSA — это линия на плоскости, задаваемая уравнением $y^2=x^3+a\cdot x+b$.

Чтобы создать подпись, сообщение сначала хэшируется и затем используется приватный ключ для создания эллиптической кривой. Затем используется публичный ключ для расшифровки кривой и проверки подписи.

Принцип стойкости ECDSA основывается на “односторонних функциях”, потому что дискретный логарифм на эллиптических кривых очень труден для вычисления. Кроме того, алгоритм имеет высокую скорость работы и меньшее потребление ресурсов, что делает его идеальным для использования в мобильных устройствах и других устройствах с ограниченными ресурсами.

Сети Bitcoin и Ethereum используют эллиптическую кривую secp256k1 [3], уравнение которой $y^2=x^3+7$, определенную в стандарте эффективной криптографии и точку G(x,y), такую, что:

$$x = 79BE667EF9DCBBAC55A06295CE870B07029BFCDB2DCE28D959F2815B16F81798$$

$$y = 483ADA7726A3C4655DA4FBFC0E1108A8FD17B448A68554199C47D08FFB10D4B8$$

На рисунке 2 изображена эллиптическая кривая $y^2=x^3+7$:

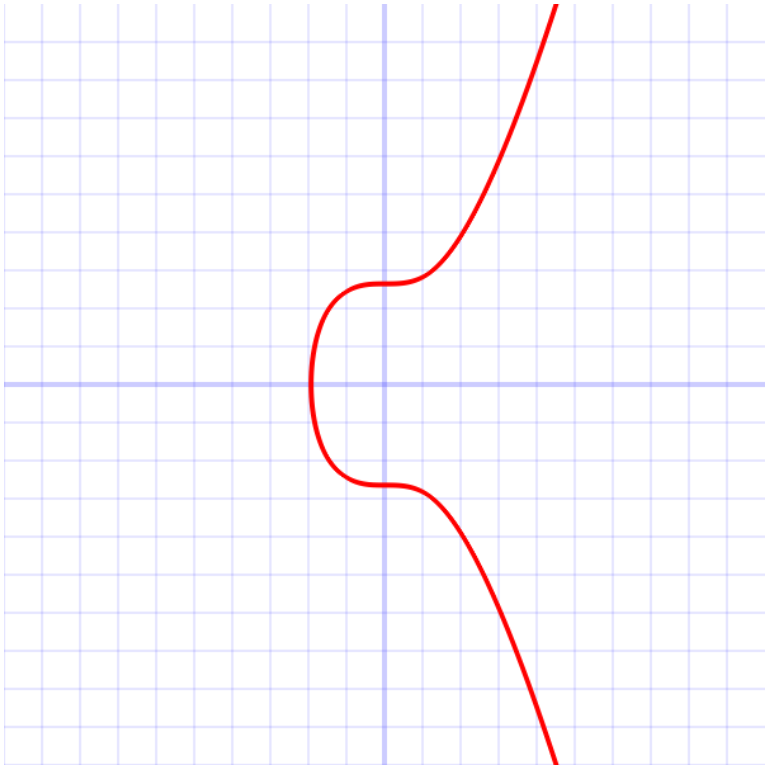

Рисунок 2 – Эллиптическая кривая $y^2=x^3+7$

Алгоритм доказательства доли владения (Proof-of-Stake) [4] используется в сети Ethereum в качестве механизма консенсуса участников сети для подтверждения транзакций, т. е. создания и передачи невзаимозаменяемых токенов. Суть алгоритма доказательства доли владения заключается в том, что владельцы криптовалюты могут ставить свою криптовалюту в залог в обмен на возможность быть выбранными для создания новых блоков и получения вознаграждения. Чем больше криптовалюты у участника сети в залоге, тем больше шансов у него быть выбранным. Ставки используются при подписи транзакций, и владелец криптовалюты гарантирует ценой своей ставки целостность и подлинность транзакции.

Изначально сеть Ethereum работала используя механизм доказательство выполнения работы (Proof-of-work). При таком подходе участники сети решают задачи на нахождение простых чисел на больших диапазонах для подписи транзакций используя вычислительные мощности и получают за это вознаграждение в виде криптовалюты. При PoS нет необходимости решать сложные математические задачи, что снижает затраты на электроэнергию и вычислительную мощность. Кроме того, PoS считается более безопасным, так как для атаки на сеть нужно контролировать более 50% криптовалюты, что значительно сложнее, чем контролировать более 50% вычислительной мощности.

Однако, PoS не лишен недостатков. Например, стейкеры могут быть не заинтересованы в обеспечении безопасности сети, так как они получают вознаграждение, даже если они не участвуют в создании блоков. Также, у PoS есть потенциальные проблемы с распределением криптовалюты, так как владельцы большого количества криптовалюты могут получать еще больше криптовалюты в виде вознаграждения.

При алгоритме доказательства доли владения, в отличие от варианта доказательства майнингом, нет необходимости решать сложные математические задачи, что снижает затраты на электроэнергию и вычислительную мощность. Схема алгоритма доказательства доли владения изображена на рисунке 2:

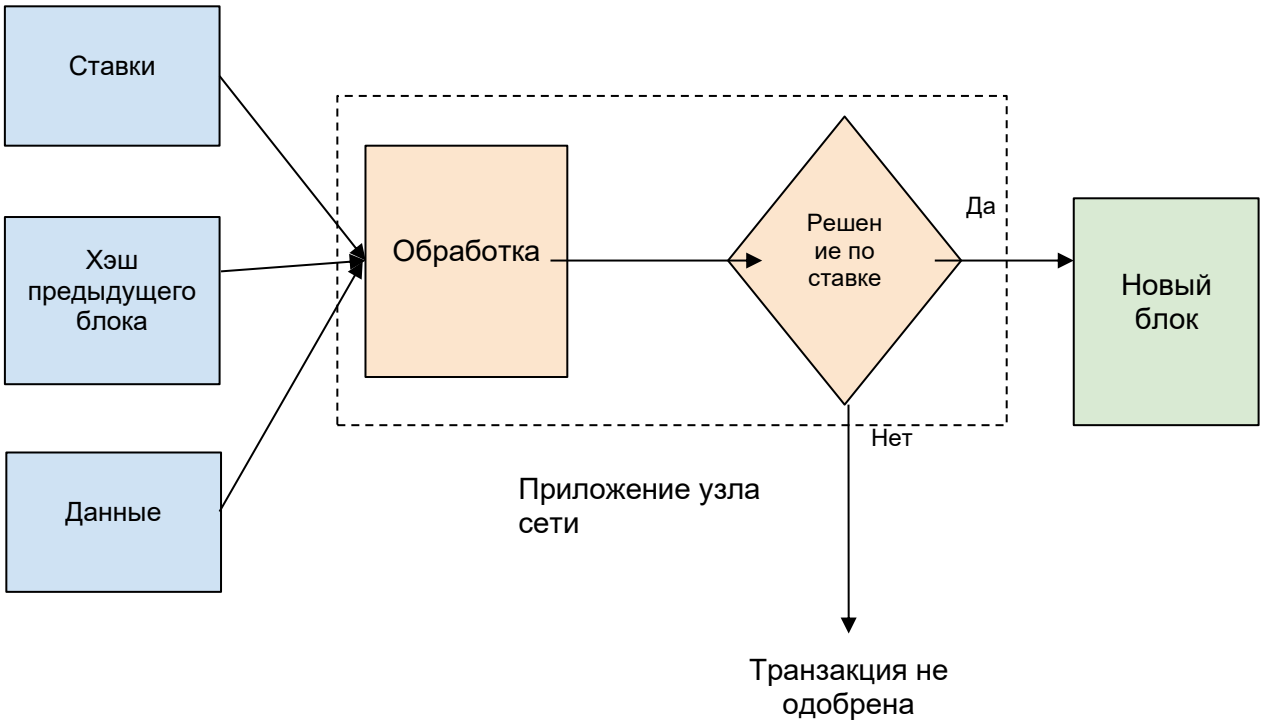

Рисунок 2 – Алгоритм доказательства доли владения

Таким образом, для проверки криптографической стойкости NFT необходимо провести аудит кода смарт-контракта на предмет использования надёжных алгоритмов хэширования SHA и эллиптические кривых для цифровых подписей, а также рассмотреть механизм консенсуса сети.

Были исследованы используемые криптографические алгоритмы в децентрализованных приложениях с использованием смарт-контрактов Ethereum, проанализирован стандарт ERC 721 с точки зрения криптографической стойкости. Было дано обоснование криптографической стойкости NFT на базе смарт-контрактов Ethereum — использование надежных алгоритмов хэширования, цифровой подписи и алгоритма доказательства доли владения делает смарт-контракт стойким к атакам на подмену содержимого блоков, редактированию токенов и краже.

Разработана методика проверки надежности кода смарт-контракта NFT. Исходный код необходимо проверить на факт соответствия стандарту ERC 721, использования алгоритмов хэширования семейства SHA, использования алгоритма цифровой подписи на основе эллиптических кривых и использования алгоритма доказательства доли владения в целевой сети развертываемого приложения.

Список использованных источников:

1. *ERC 721: Non-fungible Token standard [Electronic resource] / Ethereum foundation, 2018. – Mode of access: https://eips.ethereum.org/EIPS/eip-721. – Date of access : 20.03.2023.*

2. *Виды атак на блокчейн и умные контракты / Трубач Г. Г. // 75-я научная конференция студентов и аспирантов Белорусского государственного университета: материалы конф. В 3 ч. Ч. 2, Минск, 14–23 мая 2018 г. Белорус. гос. ун-т, Гл. упр. науки – 2018. – С. 278-281.*

3. *Arithmetic of Koblitz Curve Secp256k1 Used in Bitcoin Cryptocurrency Based on One Variable Polynomial Division / Santoshi Pote, Virendra Sule, B.K. Lande // 2nd International Conference on Advances in Science & Technology (ICAST) 2019 on 8th, 9th April 2019 by K J Somaiya Institute of Engineering & Information Technology, Mumbai, India. – 2019. – p. 333-338.*

4. *Proof-of-Stake consensus mechanism [Electronic resource] / Ethereum foundation, 2022. – Mode of access: https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/. – Date of access : 20.03.2023.*

UDC 621.3.049.77–048.24:537.2

JUSTIFICATION OF CRYPTOGRAPHIC STRENGTH OF NFT BASED ON ETHEREUM SMART CONTRACTS

Pletinskij I.V.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus
Nesterenkov S.N. – PhD in echnical Sciences

Annotation. The ERC 721 standard for non-interchangeable tokens based on Ethereum smart contracts and technical documentation were studied. Cryptographic algorithms used, data structures and transaction validation algorithms in the blockchain were studied. The cryptographic robustness of NFT based on Ethereum smart contracts was justified. A methodology for auditing NFT smart contract code was developed.

Keywords. NFT, ERC 721, smart contract, SHA-256, elliptic curves, proof of stake