УДК 519.688

# ПРОЕКТИРОВАНИЕ И РАЗРАБОТКА ОБУЧАЮЩЕГО БЛОКЧЕЙН-СИМУЛЯТОРА

**О. М. Меховников[1] [0009-0008-5247-7341], А. С. Тощев[2] [0000-0003-4424-6822]**

[1, 2] *Институт информационных технологий и интеллектуальных систем, Казанский (Приволжский) федеральный университет, ул. Кремлевская, 35, г. Казань, Республика Татарстан 420008*

[1]oleg_mekhovnikov@mail.ru, [2]atoschev@kpfu.ru

***Аннотация***

Представлен блокчейн-симулятор, предназначенный для обучения студентов и начинающих блокчейн-разработчиков. Симулятор создан с целью предоставить пользователям интуитивно понятное и доступное средство для изучения основных концепций и механизмов функционирования блокчейна. Рассмотрены основные аспекты проектирования и архитектуры симулятора, а также представлена демонстрация работы приложения. Разработанный симулятор способствует привлечению новых специалистов в сферу блокчейн-разработки.

***Ключевые слова**: блокчейн, блокчейн-симулятор, введение в блокчейн*

## ВВЕДЕНИЕ

Актуальность работы продиктована ростом популярности технологии блокчейн и, как следствие, потребностью в подготовке специалистов в этой области. В ходе исследования было выявлено, что существующие симуляторы, а именно, Bitcoin Simulator [1], BlockSim: Faria [2], SimBlock [3], BlockSim: Alharby [4] и VIBES [5], мало пригодны для целей обучения, так как работают по принципу «черного ящика» и не дают возможности просматривать данные отдельно взятого блока, транзакции и те данные, которые временно хранятся на узле до включения в блокчейн (например, транзакции из пула узла). Таким образом, возникает потребность в создании нового симулятора, который будет обеспечивать

прозрачность потока данных и наглядно демонстрировать принципы работы блокчейн-сети.

## АРХИТЕКТУРА БЛОКЧЕЙН-СИМУЛЯТОРА

Архитектура симулятора представляет собой многослойную структуру модулей (рис. 1). Рассмотрим каждый из представленных слоев.

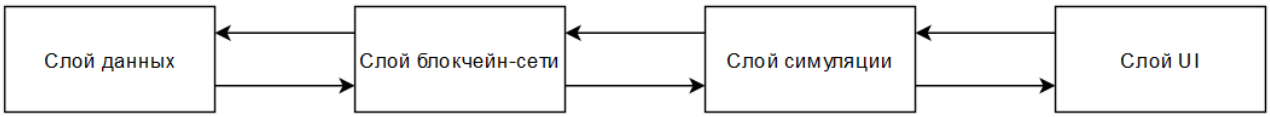


Рис. 1. Поток данных в многослойной архитектуре

Слой данных инкапсулирует модель блокчейна. В целях достижения наибольшей прозрачности работы системы данный слой был несколько упрощен в сравнении с Bitcoin [6]. В частности, были вырезаны такие механизмы, как деревья Меркла [7], упрощенная проверка платежей [6] и UTXO [6]. В этих же целях были упрощены структуры данных блокчейна. Для сравнения: диаграмма классов блокчейна, построенная по данным реального блока Bitcoin [8], представлена на рис. 2.

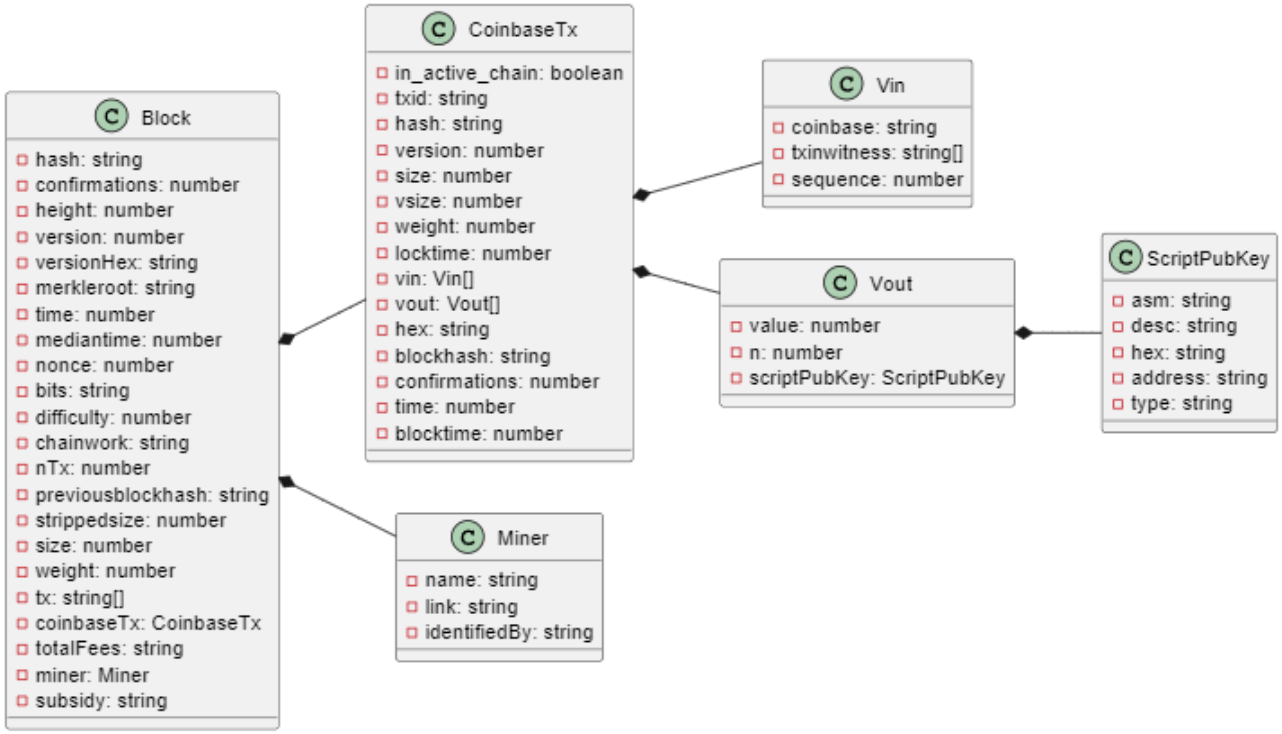


Рис. 2. Диаграмма классов блокчейна Bitcoin

Диаграмма классов блокчейна разработанного симулятора представлена на рис. 3.

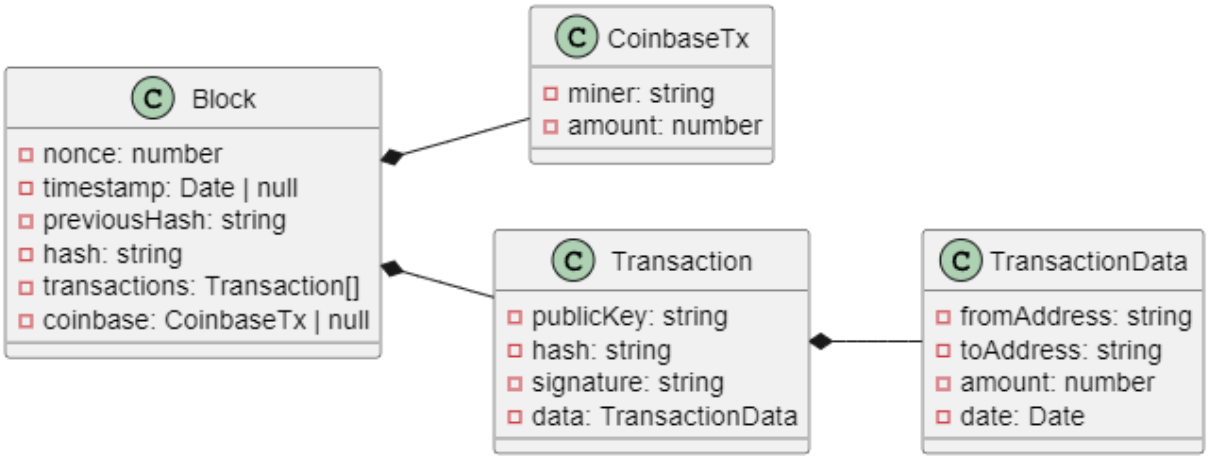


Рис. 3. Диаграмма классов блокчейна

Слой блокчейн-сети инкапсулирует логику работы сети, аналогичной Bitcoin с незначительными изменениями:

- Новые транзакции рассылаются всем узлам.
- Каждый узел включает полученные транзакции в блок.
- Узлы выбирают случайный nonce и находят хэш блока.
- Как только узлу удается найти подходящий хэш, он отправляет блок в сеть.
- Узлы принимают блоки только в том случае, если все транзакции в них корректны и не повторяются.
- Узлы выражают согласие с новыми данными, начиная работу над следующим блоком и используя хэш предыдущего блока в качестве новых исходных данных.

Слой симуляции отвечает за моделирование процесса обмена транзакциями между участниками сети. Симуляция реализована по принципу дискретно-событийного моделирования: генератор случайных чисел возвращает число, определяющее следующее событие, которое будет обработано системой (рис. 4).

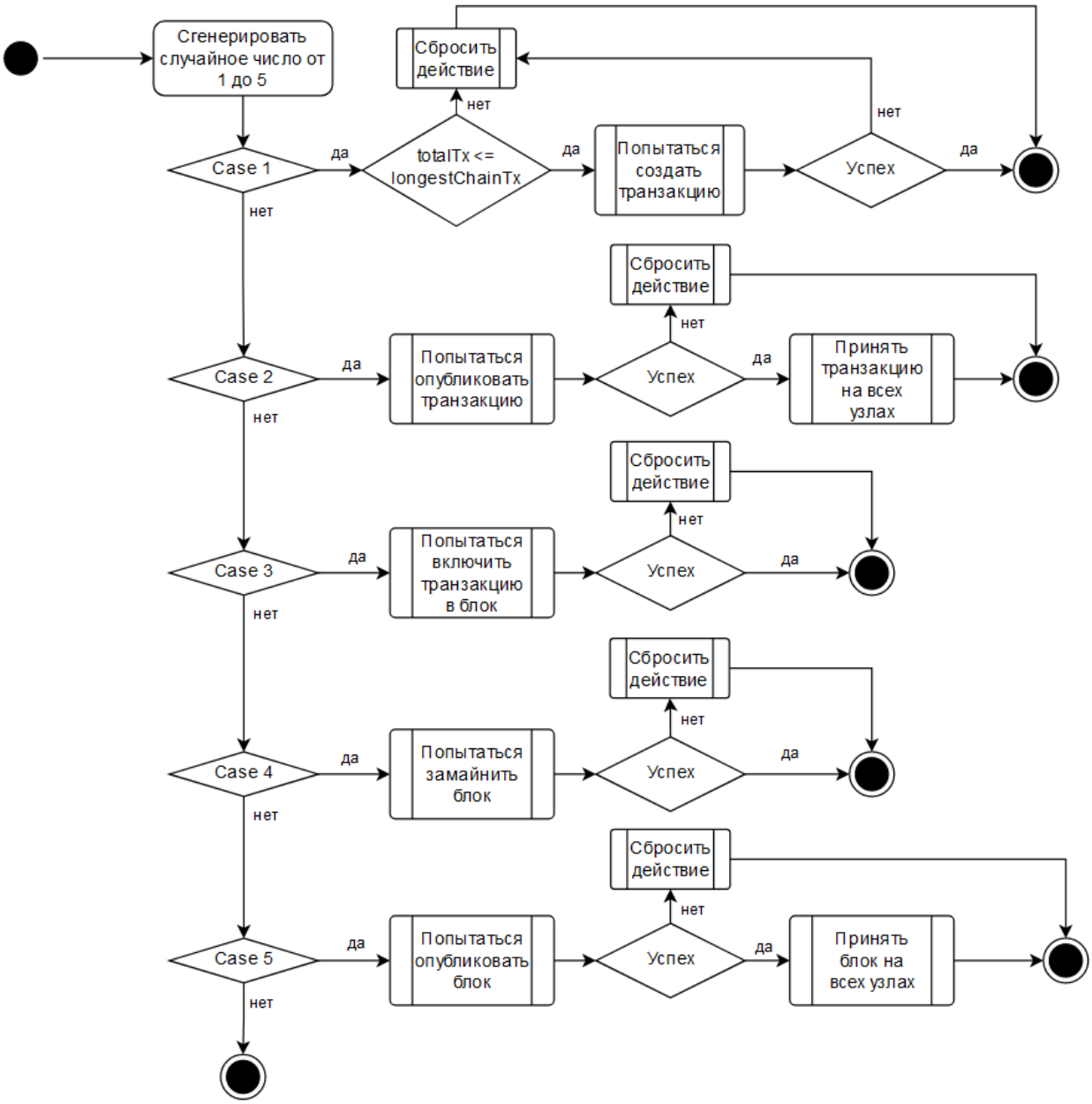


Рис. 4. Блок-схема алгоритма симуляции

**totalTx** – общее число совершенных транзакций.

**longestChainTx** – число транзакций в самом длинном блокчейне.

Слой UI включает в себя такие компоненты, как сетевая диаграмма, лог операций, список узлов, миниатюра блокчейна, модальные окна блока и узла и т. д.

## ДЕМОНСТРАЦИЯ РАБОТЫ БЛОКЧЕЙН-СИМУЛЯТОРА

Программа принимает на вход файл в формате JSON, описывающий массив узлов. В текущем примере блокчейн каждого узла представлен одним блоком, который содержит единственную coinbase-транзакцию, которая начисляет 10000 BTC на адрес, связанный с данным узлом (листинг 1).

```
{
        "id": 1,
        "name": "Узел 1",
        "publicKey":
"04ebe3074d1fe1c97a1385a2644856085815d592b4f7db1eb71e3faff6f64694c2d97815c8cf5c5
b6979083e487231fbb3bd6968f62d09c81056ea2fc9ec73ffd2",
        "privateKey":
"3503c1dbc9712c3f7cb22b167479c371770ab60ece3b4f7c22994be33187d24b",
        "blockchain": {
            "chain": [
                {
                    "nonce": 2083236893,
                    "previousHash":
"0000000000000000000000000000000000000000000000000000000000000000",
                    "hash":
"3f5b126e860591a11402e6899ea5a5e88343df767aa5800168a10f6b4df31ec1",
                    "transactions": [],
                    "coinbase": {
                        "miner":
"04ebe3074d1fe1c97a1385a2644856085815d592b4f7db1eb71e3faff6f64694c2d97815c8cf5c5
b6979083e487231fbb3bd6968f62d09c81056ea2fc9ec73ffd2",
                        "amount": 10000
                    }
                }
            ]
        },
        "transactionPool": [],
        "newBlock": null,
        "newTransaction": null
    }
```

Листинг 1. Входные данные для Узла 1.

В текущей реализации параметры блокчейна устанавливаются через программный код. Для данного примера была задана следующая конфигурация:

- Количество транзакций в блоке = 3.
- Вознаграждение за майнинг = 10 BTC.

Рассмотрим процесс работы симулятора. После завершения загрузки приложения и чтения входных данных из файла главный экран программы выглядит следующим образом (рис. 5.)

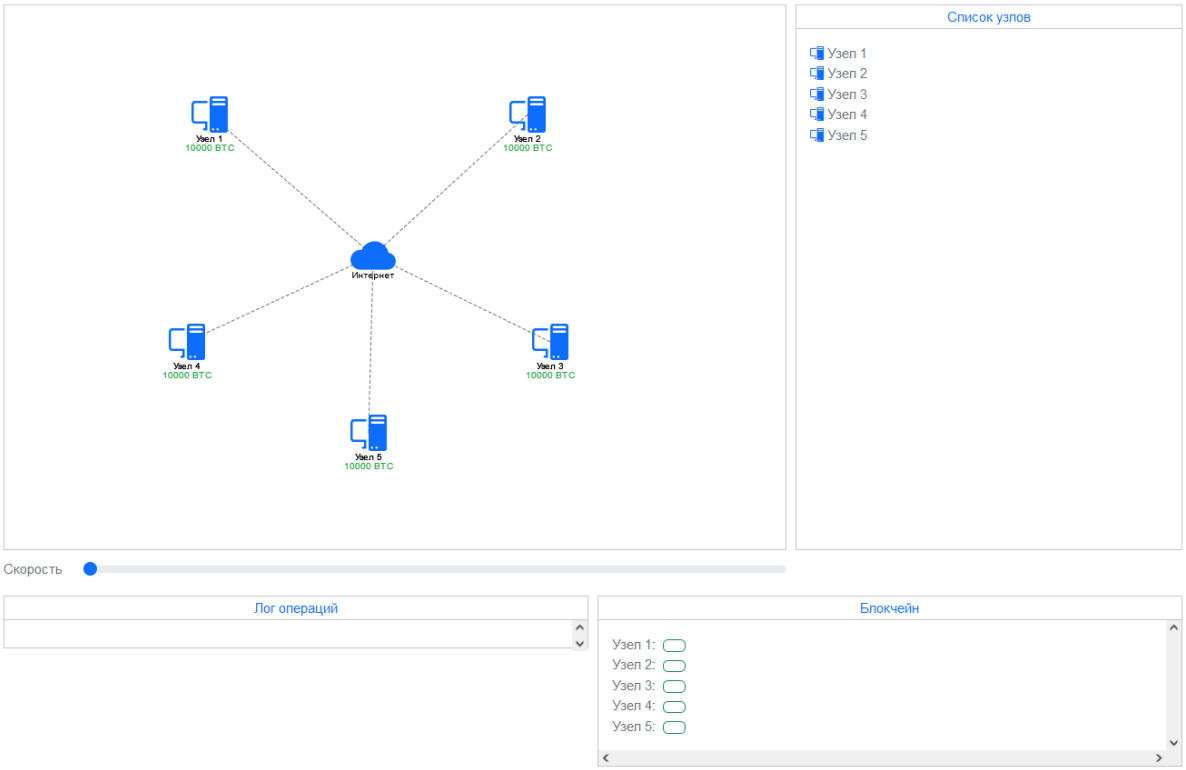


Рис. 5. Главный экран программы после загрузки входных данных

Далее узлы начинают обмениваться криптовалютными транзакциями и генерировать блоки. Сгенерированные блоки отображаются в компоненте Блокчейн (рис. 6).

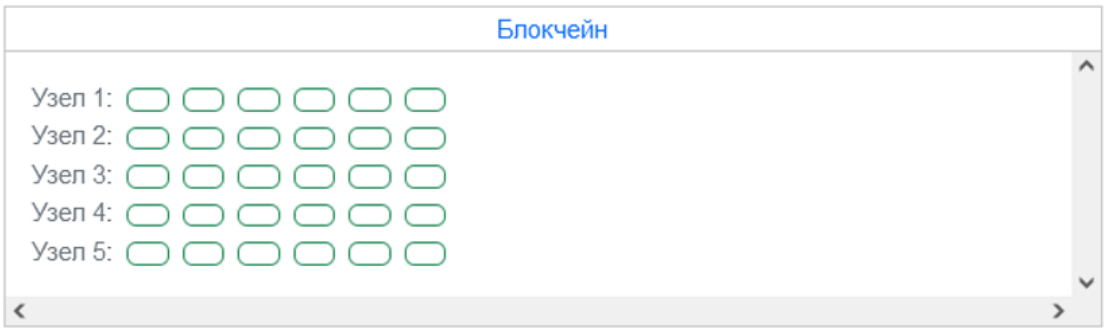


Рис. 6. Блокчейн после генерации 5 блоков

Данный компонент отображает схему копий блокчейна, хранящихся на каждом узле. Симулятор предоставляет возможность просмотра данных каждого блока, включая его транзакции, при выборе соответствующего блока в блокчейне (рис. 7).

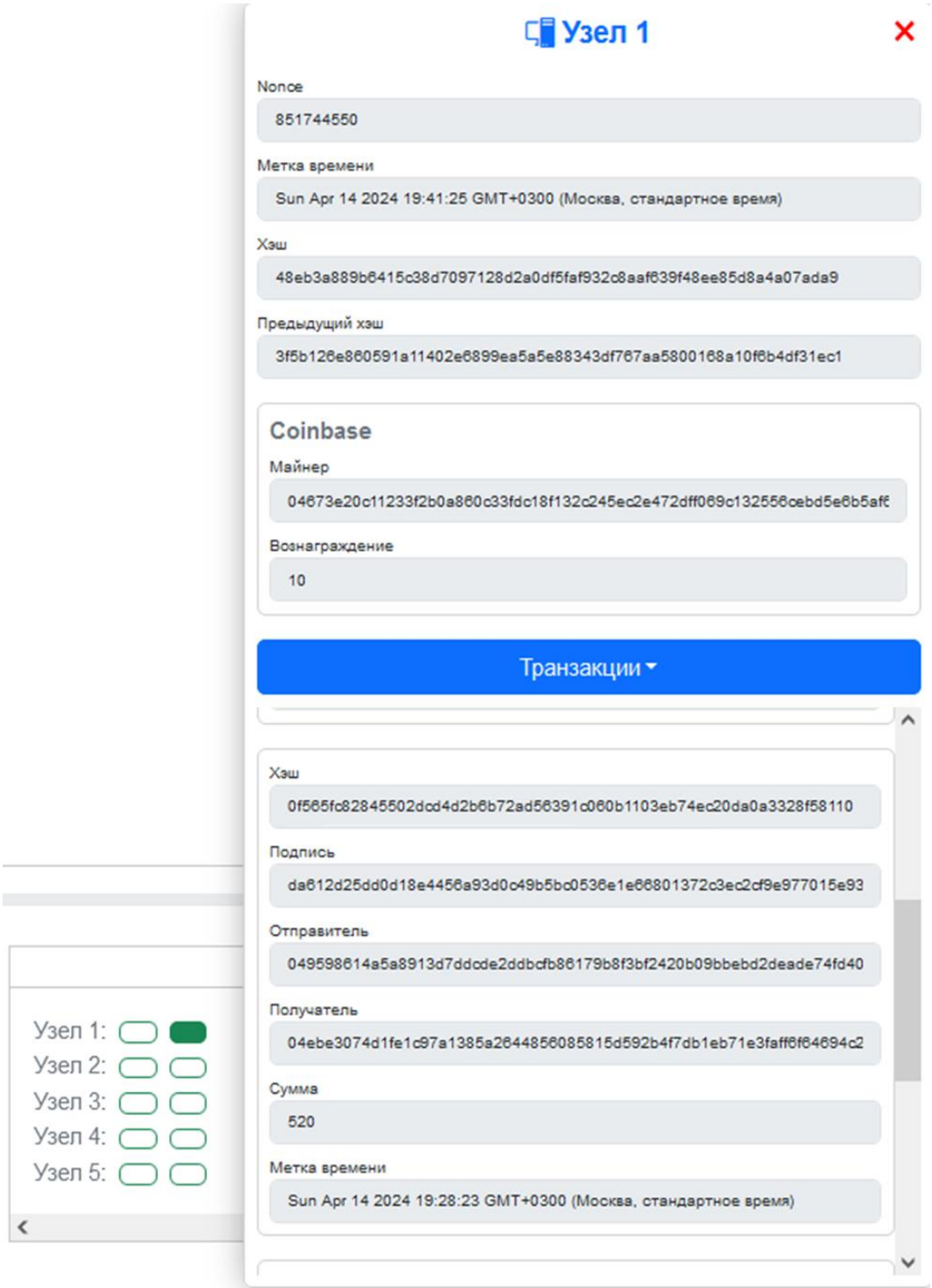


Рис. 7. Просмотр блока

В ходе симуляции через равные промежутки времени происходит одно из событий: *Транзакция создана, Транзакция распространяется по сети, Транзакция попадает в пул узла, Транзакция попадает в блок, Новый блок сгенерирован, Новый блок распространяется по сети, Новый блок добавляется к блокчейну узла, Новый блок отброшен узлом.* Для пользовательского вывода событий предусмотрены два компонента: Лог операций и Сетевая диаграмма.

В лог операций отображается информация о 1000 последних событий, произошедших в системе (рис. 8).

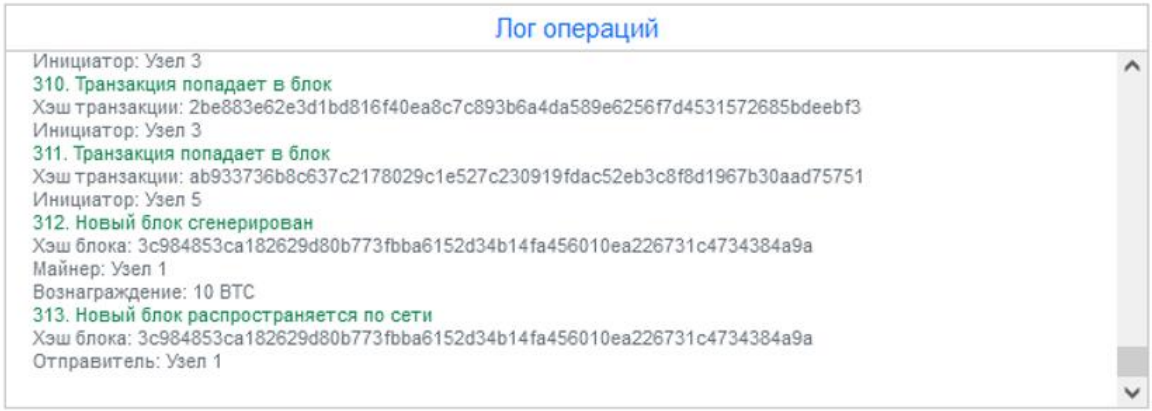


Рис. 8. Лог операций после генерации 5 блоков

Сетевая диаграмма служит для анимированного отображения событий, которые происходят в системе в данный момент (рис. 9).

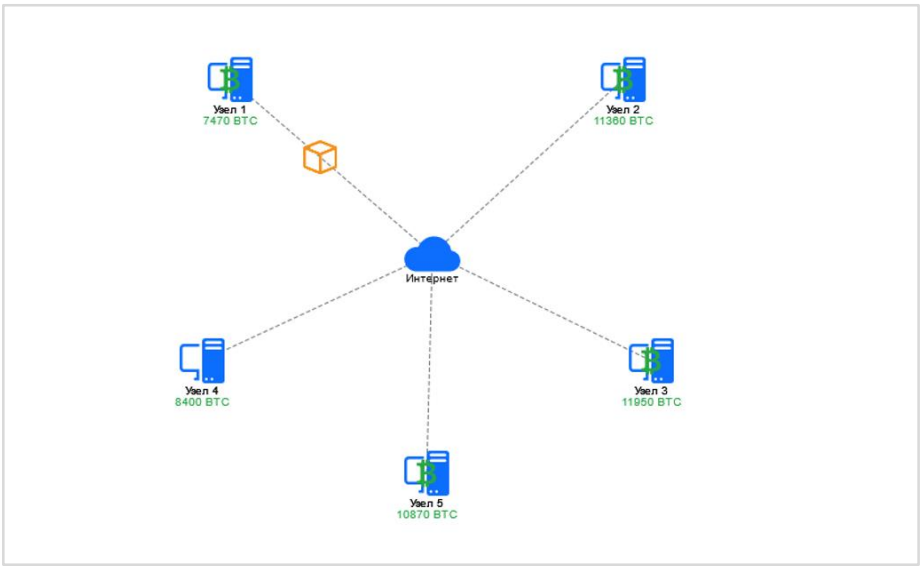


Рис. 9. Сетевая диаграмма после генерации 5 блоков

К примеру, на данном снимке на сетевой диаграмме отображены два события: *Новый блок распространяется по сети, Транзакция попадает в пул узла.*

При наступлении событий также в реальном времени обновляются следующие данные в соответствующих компонентах пользовательского интерфейса: *Блоки блокчейна, Транзакции блокчейна, Текущая неопубликованная транзакция узла, Пул транзакций узла, Текущий неопубликованный генерирующийся блок узла.*

Рассмотрим результаты симуляции: в ходе работы приложения было сгенерировано 15 транзакций, которые были включены в 5 новых блоков. Анализ выходных данных показал, что получившийся на выходе снимок состояния блокчейн-сети является полностью валидным.

## ЗАКЛЮЧЕНИЕ

В результате исследования спроектирован и разработан обучающий блокчейн-симулятор, который включает в себя основные компоненты и механизмы реального блокчейна. Симулятор позволяет пользователям ознакомиться с такими ключевыми аспектами технологии блокчейн, как создание транзакций и формирование блоков.

Эксперимент показал, что разработанный симулятор способен не только корректно моделировать блокчейн-сеть, но и в удобном виде предоставлять информацию о событиях, происходящих в системе.

Существенным преимуществом симулятора является то, что его может запустить в браузере любой желающий. Симулятор может быть использован в качестве учебного материала при обучении технологии блокчейн. Например, его можно демонстрировать студентам высших учебных заведений при освоении соответствующих образовательных программ.

## СПИСОК ЛИТЕРАТУРЫ

1. *Gervais A., Karame G.O., Wüst K., Glykantzis V., Ritzdorf H., Capkun S.* On the security and performance of proof of work blockchains // Proceedings of the 2016 ACM SIGSAC conference on computer and communications security. 2016. P. 3–16.

2. *Faria C., Correia M.* BlockSim: blockchain simulator // 2019 IEEE International Conference on Blockchain (Blockchain). IEEE, 2019. P. 439–446.

3. *Aoki Y., Otsuki K., Kaneko T., Banno R., Shudo K.* Simblock: A blockchain network simulator // IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). IEEE, 2019. P. 325–329.

4. *Alharby M., Van Moorsel A.* Blocksim: a simulation framework for blockchain systems // ACM SIGMETRICS Performance Evaluation Review. 2019. Vol. 46, No. 3. P. 135–138.

5. *Stoykov L., Zhang K., Jacobsen H.-A.* Vibes: fast blockchain simulations for large-scale peer-to-peer networks // Proceedings of the 18th ACM/IFIP/USENIX Middleware Conference: Posters and Demos. 2017. P. 19–20.

6. *Nakamoto S.* Bitcoin: A peer-to-peer electronic cash system. URL: http://www.bitcoin.org/bitcoin.pdf.

7. *Mercle R.C.* Protocols for public key cryptosystems // Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society. 1980. P. 122–133.

8. Block #838,614 | bitcoinexplorer.org.
URL: https://bitcoinexplorer.org/block-height/838614.

## DESIGN AND DEVELOPMENT OF A TRAINING BLOCKCHAIN SIMULATOR

**Oleg Mekhovnikov[1] [0009-0008-5247-7341], Alexander Toschev[2] [0000-0003-4424-6822]**

[1, 2] *Institute of Information Technologies and Intelligent Systems, KFU University, st. Kremlin, 35, Kazan, Republic of Tatarstan 420008*

[1]oleg_mekhovnikov@mail.ru, [2]atoschev@kpfu.ru

***Abstract***

This article presents an educational blockchain simulator intended for training students and beginning blockchain developers. The simulator was created to provide users with an intuitive and accessible tool for learning the basic concepts and mechanisms of blockchain functioning. The article discusses the main aspects of the design and architecture of the simulator, and also provides a demonstration of the applica-

tion. In addition, the possibilities for further development of the simulator and its potential as a tool for teaching and research in the field of blockchain technologies are discussed. The resulting simulator contributes to the field of education and science, helping to increase the level of competence of specialists and the development of innovative solutions in the field of blockchain.

***Keywords****: blockchain, blockchain simulator, introduction to blockchain*

**REFERENCES**

1. *Gervais A., Karame G.O., Wüst K., Glykantzis V., Ritzdorf H., Capkun S.* On the security and performance of proof of work blockchains // Proceedings of the 2016 ACM SIGSAC conference on computer and communications security. 2016. P. 3–16.

2. *Faria C., Correia M.* BlockSim: blockchain simulator // 2019 IEEE International Conference on Blockchain (Blockchain). IEEE, 2019. P. 439–446.

3. *Aoki Y., Otsuki K., Kaneko T., Banno R., Shudo K.* Simblock: A blockchain network simulator // IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). IEEE, 2019. P. 325–329.

4. *Alharby M., Van Moorsel A.* Blocksim: a simulation framework for blockchain systems // ACM SIGMETRICS Performance Evaluation Review. 2019. Vol. 46, No. 3. P. 135–138.

5. *Stoykov L., Zhang K., Jacobsen H.-A.* Vibes: fast blockchain simulations for large-scale peer-to-peer networks // Proceedings of the 18th ACM/IFIP/USENIX Middleware Conference: Posters and Demos. 2017. P. 19–20.

6. *Nakamoto S.* Bitcoin: A peer-to-peer electronic cash system.
URL: http://www.bitcoin.org/bitcoin.pdf

7. *Mercle R.C.* Protocols for public key cryptosystems // Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society. 1980. P. 122–133.

8. Block #838,614 | bitcoinexplorer.org.
URL: https://bitcoinexplorer.org/block-height/838614

## СВЕДЕНИЯ ОБ АВТОРАХ

***МЕХОВНИКОВ Олег Максимович*** – разработчик ПО, студент магистратуры, исследователь. Казанский федеральный университет, Казань, Россия.

***Oleg Maksimovich MEKHOVNIKOV*** – software developer, master's student, researcher. Kazan Federal University, Kazan, Russia.

email: oleg_mekhovnikov@mail.ru
ORCID: 0009-0008-5247-7341

***ТОЩЕВ Александр Сергеевич*** – доцент, к. н. , КФУ, Институт информационных технологий и интеллектуальных систем, Кафедра программной инженерии, г. Казань.

***Alexander Sergeevich TOSCHEV*** – Associate Professor, Ph.D., KFU, Institute of Information Technologies and Intelligent Systems, Department of Software Engineering, Kazan.

email: atoschev@kpfu.ru
ORCID: 0000-0003-4424-6822

*Материал поступил в редакцию 13 мая 2024 года*