

**ИМИТАЦИОННАЯ МОДЕЛЬ VOTING 2PL ПРОТОКОЛА КАК ПОДХОД К  
МОДЕЛИРОВАНИЮ БЛОКЧЕЙН ТРАНЗАКЦИЙ****Василева С.Ж. (Добрич, Болгария)**

В последние годы „набирает скорость“ новый денежный способ – т. наз. „криптовалюты“. Криптовалюты, не только упрощают процедуру посылки денежных сум, при этом все случается в границах одной (глобальной) сети [6]. Криптовалюты и блокчейн технологии имеют и другие преимущества перед классическими денежными системами: - Распределенные сети “работают” круглосуточно и без выходного дня (24/7), что позволяет отправление денежных средств в любое время; - Люди бизнеса и владельцы компаний могут без лишних расходов и намного свободнее оперировать на международном уровне.

Bitcoin является первой полностью цифровой валютой. [15] „В отличие от электронных денежных средств, он не существует даже в виде цифрового файла. Блокчейн представляется в виде гигантской книги учета, которая доступна всем участникам сети. Каждая транзакция не хранится отдельно, информация помещается в блокчейн блоках.“ [15]. “Каждый последующий блок хранит в себе информацию о предыдущем. Важной особенностью работы блокчейна является его децентрализация, так как информация одновременно хранится у всех участниках системы.” [9], [10], [15]

Единственно необходимое и достаточное условие для существования этой платежной системы- наличие программы-клиента (с открытым кодом). Сгенерированные на множестве компьютеров программы-клиенты объединяются в одноранговую сети, каждый узел которой имеет одинаковые права и является самодостаточным [10]. В этом смысле блокчейн транзакции можно моделировать с помощью алгоритмов симулирующих управление транзакций в распределенных базах данных.

Блокчейн формируется как непрерывно увеличивающимся списком блоков с записями о всех транзакциях. Каждый компьютер или устройство, включенное в блокчейн сети, получает файл со всей информацией, созданной в этой блокчейн цепи. Копия базы или ее частей сохраняются одновременно на множестве компьютеров и синхронизируются по формальным правилам (наз. протокол) для построения цепи блоков. Информация в блоках не является зашифрованной и доступна в сети, но криптографически, с помощью элементов электронной подписи удостоверяется, что нет перемен в списке и никогда большее нельзя удалить или изменить. Каждый компьютер, который подключен к блокчейн (независимо когда), может восстановить структуру и содержимое любого блока [2], [10]. Редактирование данных в блокчейне технически является невозможным, и можно только стереть путем удаления всей цепи в блокчейн.

Так как для предотвращения двойного расхода в блокчейн используются временные метки (timestamps), осуществляемые путем разбиения базы данных как структуру из специальных блоков, каждый из которых, содержит внутри себя, и хэш предыдущего блока, и свой номер, то можно придумать применить один из протоколов временных меток (конкретнее его многоверсионный вид) для создания имитационной модели на процесса исполнения блокчейн транзакций. Каждый новый блок утверждает транзакции, информацию которых он содержит и в дополнении подтверждает транзакции со всех предыдущих блоков цепи, (и применяется механизм похожий на голосование). Создается впечатление, что при создании алгоритма моделирующего блокчейн транзакций можно удачно применить протокол для блокировки большинства копий [7].

Следовательно, одним из возможных алгоритмов для моделирования исполнения блокчейн транзакций является протокол двухфазной блокировки большинства копий [7], путем применения элементов протокола временных меток [7], при этом распределенная база данных [7], [13] имеет многоверсионную структуру [7].

Поэтому для моделирования в целях исследования систем с блокчейн транзакциями в работе предлагается алгоритм моделирующий управление распределенными транзакциями, по протоколу двухфазной блокировки (Two-phase Locking – 2PL) большинства копий, так называемый Voting 2PL [6, с.988], [8] и [14]. В моделирующем алгоритме [1] данные являются неполностью

реплицированными (число копий элемента данных меньше чем число сайтов в системе). Исполнено имитационное моделирование двухфазной блокировки большинства копий для моноверсионной модели распределенной базы данных, в которой элементы данных имеют 3 копия. Имитационная модель создана средствами „классической” системы моделирования – GPSS World и конкретнее - GPSS World Personal Version [4], [5].

Имитационное моделирование систем с распределенными базами данных и распределенных транзакций

Методы имитационного моделирования (далее ИМ) дают возможность исследователям создавать модели сложных систем, что не всегда может обеспечить математическое моделирование. Эти модели могут помочь руководителям и людям начинающим или желающим сделать свою организацию более эффективной. Однако в экономике многих странах не используются столь эффективно мощные инструменты ИМ [4], [5]. Поэтому приводится пример применения системы ИМ GPSS World [5] в исследовании и совершенствовании систем с крипто валютой.

Каждая система (техническая, информационная, экономическая, социальная и др.) и алгоритм ее работы могут быть описаны в терминах теории массового обслуживания [5], и большинство из них может быть решено аналитическими методами. ИМ дает возможность исследовать систему массового обслуживания для разных типов входящих потоков и интенсивностей поступлений транзакций на входах систем и определять их основные характеристики без каких-либо допущений и ограничений [4] и [5]. Имея ввиду результаты работы [12], предлагается моделирование систем с блокчейн транзакциями осуществлять с помощью систем имитационного моделирования, таких как GPSS World[5] и GPSS Studio [3] и [4].

На рис. 1 показана модель [1] распределенной системы управления базами данных (далее РСУБД) работающей по Voting 2PL протоколу в виде системы массового обслуживания;

$S_1 - S_n$  – генераторы параллельных транзакций;

$TC_1 - TC_n$  – координаторы транзакций, находящиеся в сайтах, генерирующих транзакций. Они определяют номера сайтов, где находятся копия элементов данных. Перед устройствами моделирующими работу координаторов организованы очереди, в которых транзакции выжидают освобождение устройств обслуживания;

$QLM_1 - QLM_n$  – очереди для транзакций, где они выжидают освобождение соответствующего устройства обслуживания, моделирующего соответствующего диспетчера блокировок;

$LM_1 - LM_n$  – диспетчеры блокировок копий элементов данных, находятся в сайтах, где тиражированы копия элементов данных;

$LT_1 - LT_n$  – таблицы блокировок соответствующих диспетчеров блокировок;

$DM_1 - DM_n$  – диспетчеры данных;

$TM_1 - TM_n$  – менеджеры транзакций, они расположены в сайтах, генерирующих транзакции и объединяют подтранзакции глобальных транзакций.

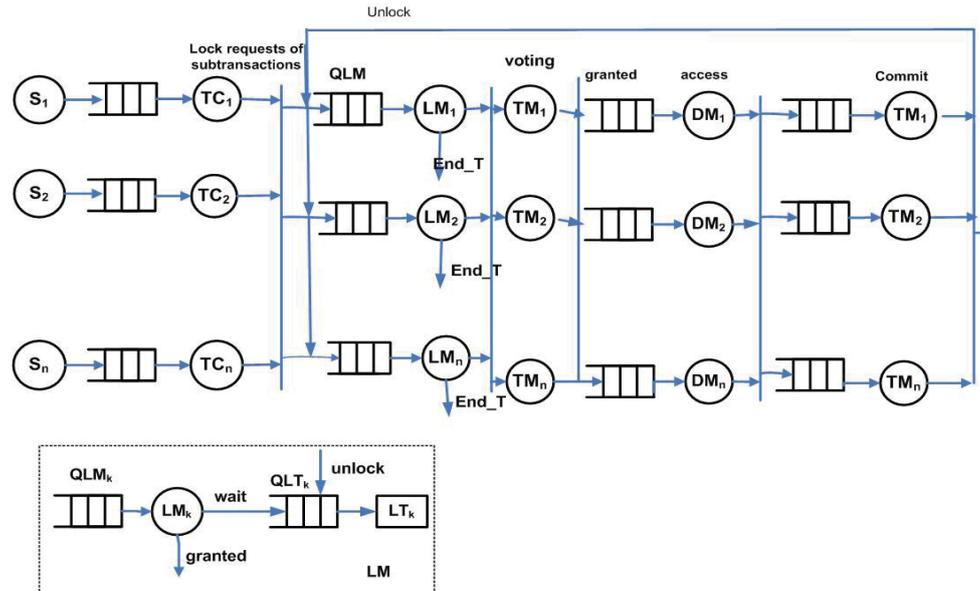


Рис. 1 Модель РСУБД работающей по Voting 2PL протоколу

В описанной модели [1] число сайтов-генераторов транзакций - 6 ( $S_1 - S_6$ ), соответствующим образом в каждый из них поступает один поток транзакций, моделированными с помощью GPSS транзактов, которые управляются соответствующими менеджерами транзакций ( $TM_1 - TM_6$ ). Так как РСУБД работает по протоколу двухфазной блокировки большинства копий, поэтому запросы на блокировку (или на освобождении блокировки) высылаются как операции транзактов к соответствующим диспетчерам блокировок  $LM_i$ .

Алгоритм двухфазной блокировки большинства копий

Основным компонентом систем управления базами данных, осуществляющими управление параллельного доступа транзакций к общим данным является организатор заданий. [7] Когда организатор совершает 2PL протокол, называется диспетчером блокировок (lock manager - LM). В случае когда РСУБД работает по Voting 2PL протокол, на каждом узлу системы имеется диспетчер блокировок LM и соответственно одна таблица блокировок (lock table - LT), которые управляют синхронизацию копий реплицированных элементов данных. Если транзакция хочет прочесть или записать элемент данных, имеющий копия в  $n$  узлах системы, она должна запросить блокировку этого элемента у больше чем половины ( $n/2$ ) узлов, где имеются копия этого элемента. Транзакция не может продолжить свое исполнение, пока не поставит блокировку большинства копий этого элемента данных. Если она не успеет сделать это в заранее установленном сроке, она отменяет свои запросы и информирует всех узлы об отмене исполнения. Если большинство подтверждений о блокировке получены, то все узлы информируются, что достигнут нужный уровень блокировки. Общая блокировка ( $rl$ ) большинства копий может быть установлена одновременно всеми транзакциями, а исключительная блокировка ( $xl$ ) - только одной транзакцией.

На рис. 2 представлена структурная схема моделирующего алгоритма исполнения глобальной (распределенной) транзакции инициированной с сайта  $S_{P2}$ , обрабатывающей элемент  $x$ , имеющий копия в локальных базах данных  $LDB_{P6}$ ,  $LDB_{P7}$  и  $LDB_{P8}$ , соответственно размещенных на сайтах  $S_{P6}$  и  $S_{P7}$  и  $S_{P8}$ . Модель создана на основе алгоритма, описанного в [14].

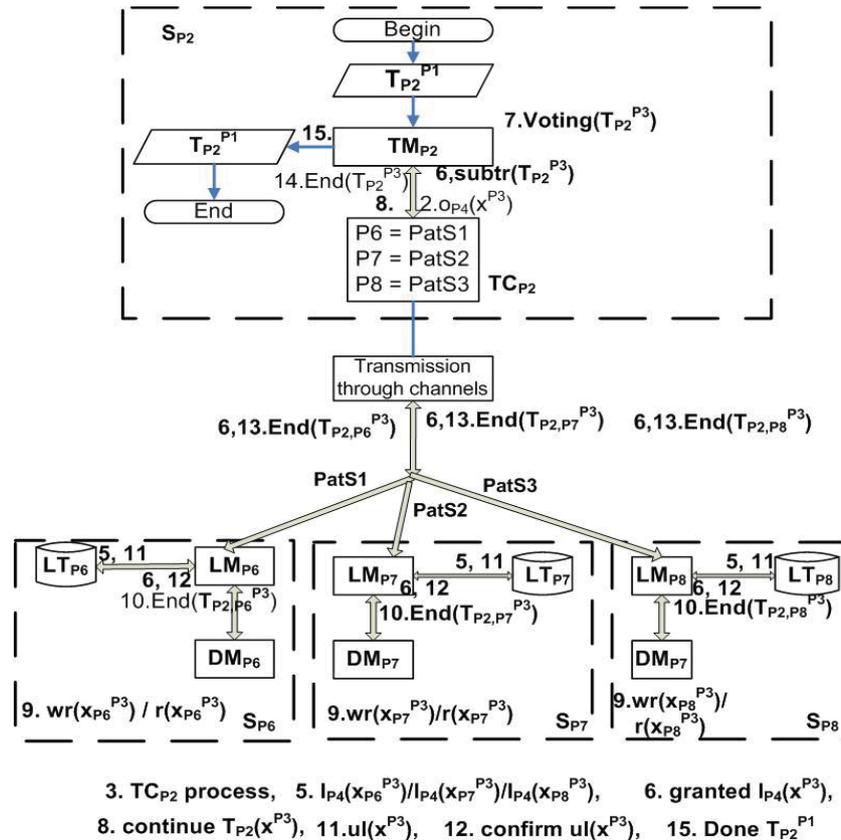


Рис. 2 Схема алгоритма, моделирующего исполнение Voting 2PL простых транзакций

Координатор транзакций  $TC_{P2}$  расщепляет „глобальный” транзакт на подтранзакты, в зависимости от того, где находятся копия обрабатываемых транзакцией элементы данных. В примере, транзакт  $T_{P2}^{P1}$  обрабатывает элемент данных копиями в локальных базах данных на сайтах  $S_{P6}, S_{P7}$  и  $S_{P8}$ , следовательно координатор транзакций расщепляет  $T_{P2}^{P1}$  на подтранзакты  $T_{P2,P6}^{P1}$ ,  $T_{P2,P7}^{P1}$  и  $T_{P2,P8}^{P1}$  и „высылает их по каналам сети” к диспетчерам блокировок  $LM_{P6}, LM_{P7}$  и  $LM_{P8}$ . Передача по каналам моделируется задержанием (блоками ADVANCE), определенным матрицами RAZST и RAZDEV.

Диспетчеры блокировок  $LM_{P6}, LM_{P7}$  и  $LM_{P8}$  обрабатывают подтранзакции: если подтранзакция получила нужную блокировку, ставится соответствующая запись в таблице блокировок, моделированной матрицей LTA и GPSS транзакт расщепляется снова, при этом наследник возвращается к менеджеру глобальной транзакции в  $S_{P2}$  для участия в голосовании вместе с остальными двумя подтранзактами ( $T_{P2,P7}^{P1}$  и  $T_{P2,P8}^{P1}$ ). Иначе расщепляется и выжидает в списке ожидающих к таблице блокировок, а наследник возвращается к менеджеру транзакции в узле  $S_{P2}$  для участия в голосовании с другими подтранзактами. Выжидание моделируется GPSS пользовательскими цепями. В сегменте модели с этикеткой *ProvMaj*[1] подсчитываются голоса подтранзактов, получили ли они блокировки копий элемента данных. Счетчик, моделированный переменной *Vot* собирает „голоса” получивших блокировку подтранзакций.

### Результаты моделирования

На рис. 3 и 4 продемонстрированы результаты работы моделирующего Voting 2PL алгоритма при одинаковых увеличивающихся интенсивностях входных потоков. Обозначения:  $BroiTr$  – общее число генерированных транзактов во время моделирования,  $FixTr$  – число фиксировавших глобальных транзакций за тот же период,  $X = FixTr/Tn$  – коэффициент фиксировавших транзакций,  $Tn$  – время моделирования работы системы.  $Ps = FixTr/BroiTr$  – вероятность обслуживания транзакций.

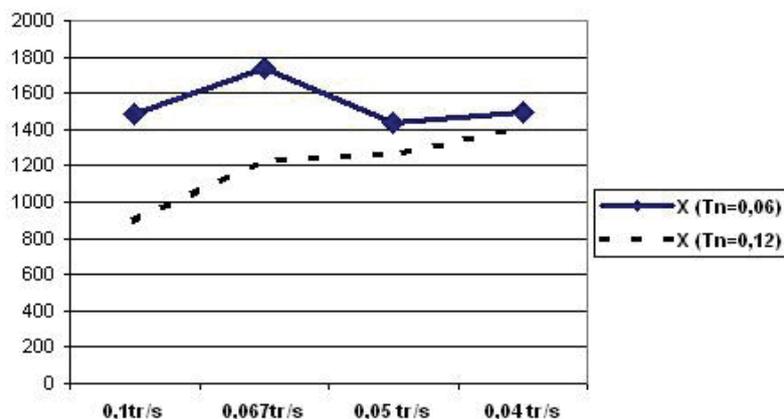


Рис. 3 Пропускная способность распределенной системы в симуляциях

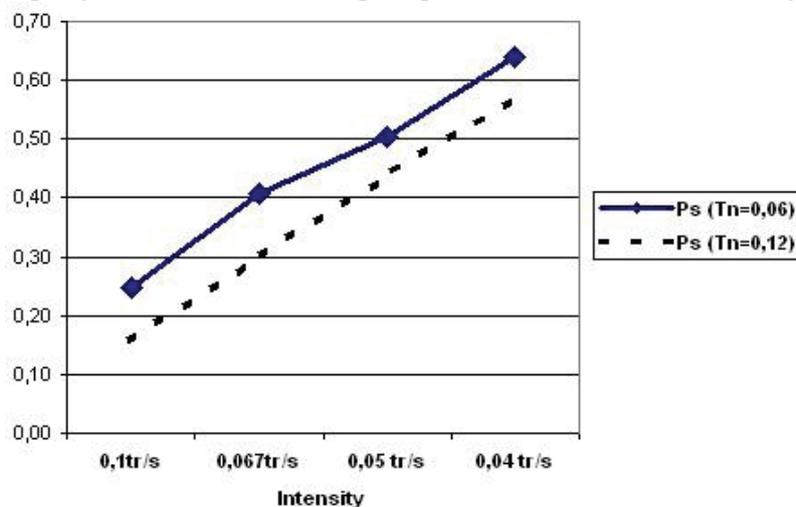


Рис. 4 Вероятность обслуживания транзакций

### Заключение

Алгоритм моделирующий Voting2PL в распределенных системах управления базами данных может быть применен в исследованиях систем с блокчейн транзакциями.

Дальнейшая работа предполагает настройка модели для сложных систем с блокчейн транзакциями. Моделирование должно быть исполнено в новой системе ИМ – GPSS Studio [3], [4]. GPSS Studio позволяет разработчику модели эффективную и быструю отладку модели с помощью отладчика, который обеспечивает не только визуальное прослеживание движения транзактов в модели, но и контроль изменения состояний и значений других объектов модели. А также конструирование интерактивных форм для анализа результатов моделирования.

### Литература

1. С.Ж.Василева, С., П. Милев. Алгоритъм модели ращ двуфазна блокировка на болшинство то копия в разпределени бази от данни. Международна Научна Конференция посветена на 105 годишнината на Джон Атанасов и 100 годишнината на Джон фон Нойман, т. 1, Шумен, 2009, с.226-233
2. Генкин, А., А. Михеев. Блокчейн. Как это работает и что ждет нас завтра. Москва, Альпина Пабlisher, <https://f.ua/alpina-publisher/blokcheyn-kak-yeto-rabotaet-i-chto-jdet-nas-zavtra-9785961465587.html>, 2017.
3. Девятков, В.В. Развитие методологии имитационных исследований сложных экономических систем. Диссертация на соискание ученой степени доктора экономических наук, Москва, РФ. <http://elib.fa.ru/avtoreferat/devyatkov.pdf/download/devyatkov.pdf>, 2015.
4. Имитационные исследования в среде моделирования GPSSSTUDIO: учеб. пособие/ В.В. Девятков, Т.В. Девятков, М.В. Федотов; под общ. ред. В.В. Девяткова. — М.: Вузовский учебник: ИНФРА-М, 2018. — 283 с.

5. Томашевский, В.Н., Жданова, Е.Г. Имитационное моделирование в среде GPSS. Бестселлер, Москва, 2003. – 416 с.
6. BITSIDE. Как построить бизнес-модель по принципу блокчейн? <https://bitside.org/kak-postroit-biznes-model-po-printsipu-blokchejn/>, 2019.
7. Connolly, T., C. Begg. Database systems. A practical Approach to Design, Implementation, and Management. Addison-Wesley, 2003.
8. Kaur, M. Transaction processing in Distributed Databases. <http://www.rimtengg.com/coit2007/proceedings>.
9. Marco, I., K. Lakhani. The Truth About Blockchain, Harvard Business Review (January–February 2017 issue), 2017, pp. 118-127.
10. Mazonka, O. Blockchain: Simple Explanation, 2016, <http://jrxv.net/x/16/chain.pdf>
11. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, <https://bitcoin.org/bitcoin.pdf>
12. Piriou, P., J. Dumas. Simulation of stochastic blockchain models, 2018 14th European Dependable Computing Conference (EDCC), 10-14 Sept. 2018, Iasi, Romania, 2018, pp. 150-157. <https://ieeexplore.ieee.org/document/8530776>
13. Srinivasa, R., C. Williams, P. Reynolds, Distributed Transaction Processing on an Ordering Network, Technical Report CS-2001-08, February 2001, p. 20, <http://citeseer.ist.psu.edu/cache/papers/cs/26119/ftp:zSzzSzftp.cs.virginia.edu/zSzpubzSztechreportszSzCS-2001-08.pdf/srinivasa01distributed.pdf>
14. Vasileva, S., P. Milev. Problems in transaction concurrency control algorithms. Tensor, N.S., Vol.67, No.3, 2006, pp.259-269.
15. <https://thecoinshark.net/ru/blockchain-transaction-how-do-they-work-and-how-to-track-them-ru/>