Научная статья
Original article
УДК 336.743
DOI 10.55186/26584964_2022_5_3_2

АЛГОРИТМЫ ДОСТИЖЕНИЯ КОНСЕНСУСА В БЛОКЧЕЙН СИСТЕМЕ

ALGORITHMS FOR REACHING CONSENSUS IN THE BLOCKCHAIN SYSTEM

Чахкиев Магомед Темирланович, Студент 2 курс, факультет, Информатика и системы управления", МГТУ им.Н.Э.Баумана, Россия, г.Москва

Chakhkiev Magomed Temirlanovich, 2nd year student, Faculty of Informatics and Control Systems, MSTU Bauman, Russia, Moscow

Аннотация: В статье анализируются алгоритмы достижения консенсуса в блокчейн системе. Рассматриваются гарантии, обеспечения которых требует консенсус в распределённой системе, и основные группы свойств алгоритмов достижения консенсуса. Приводятся общие функции механизмов консенсуса, наиболее распространённые разновидности алгоритмов достижения консенсуса, их краткие характеристики и недостатки. Выявляются требования, предъявляемые к новым алгоритмам достижения консенсуса в распределённых системах.

Аннотация: В статье анализируются алгоритмы достижения консенсуса в оценке поведения. Рассмотрены гарантии, требующие консенсуса в распределенной системе, и основные свойства групп алгоритмов достижения

консенсуса. При использовании общих функций консенсуса наиболее часто используются различные алгоритмы достижения консенсуса, их краткие характеристики и результаты. Выявляются требования, предъявляемые к новым алгоритмам, достижения консенсуса в распределённых группах.

Ключевые слова: блокчейн, распределённая система, консенсус, алгоритмы консенсуса, логика алгоритма консенсуса.

Ключевые слова: закономерность, распределённая система, консенсус, алгоритмы консенсуса, логика алгоритма консенсуса.

Введение

Развитие блокчейн систем осуществляется в направлении повышения безопасности и скорости работы и совершенствования пользовательских интерфейсов [1]. По мере появления новых систем расширяется и спектр их применения. Так, блокчейн может использоваться для контроля выполнения финансовых операций, управления предприятием, компанией или беспроводной связью, хранения авторских прав и прав собственности. Высокий уровень защищённости блокчейн системы обеспечивается алгоритмами достижения консенсуса, посредством которых достигается единое решение всех участников сети [2]. Каждый из существующих протоколов имеет свои сильные и слабые стороны, поэтому при их выборе требуется проведение тщательного ситуационного анализа, что делает актуальным исследование алгоритмов достижения консенсуса.

Целью работы является изучение алгоритмов достижения консенсуса в блокчейн системе. Для её достижения были использованы методы анализа и синтеза научных публикаций и литературных источников по рассматриваемой теме.

Свойства алгоритмов достижения консенсуса

Алгоритм достижения консенсуса является основой функционирования технологии блокчейн [3]. Благодаря ему обеспечивается высокая адаптивность системы к отключению в случайные моменты времени и её живучесть,

обусловленная автоматическим установлением новых соединений в виде распределённого доверия. Консенсус в распределённой системе требует обеспечения двух ключевых гарантий [4]:

• гарантия надёжности: все принимаемые договорённости окончательны даже при условии потенциально ненадёжного окружения;

• гарантия прогресса: в результате договорённость будет достигнута.

В блокчейн системах достижение консенсуса сводится к решению задачи о византийских генералах, которая имеет следующую формулировку [5]:

Византийская армия включает n легионов, которыми управляют отдельные генералы, подчиняющиеся главнокомандующему. Армии требуется напасть на город, поэтому она окружает его. Исход войны определяется действиями всех генералов, которым необходимо связаться с целью принятия единого решения о наступлении. При этом среди командующих могут находиться предатели, рассылающие приказы различного содержания любым генералам.

Решение этой задачи, в которой достижение консенсуса является крайне непростым, легло в основу математической модели построения и развития технологии блокчейн. В распределённых сетях отсутствует центральный орган, обеспечивающий одинаковую работу удалённых узлов, в связи с чем появляется потребность в протоколах, способных обеспечить консенсус между всеми распределёнными узлами.

Для алгоритмов достижения консенсуса выделяют четыре основные группы свойств [6]:

1. Структурные свойства. Характеризуют узловую структуру сети, участвующую в процессе достижения консенсуса. Эта группа включает:

a) типы узлов;

b) тип структуры:

• одиночный комитет: открытый или закрытый тип, явное или неявное формирование, статическая или динамическая конфигурация;

• множественный комитет: иерархическая или плоская структура, статическая или динамическая конфигурация;

c) базовый механизм определения ключевых узлов:

• вероятностный или рандомизированный механизм лотереи;

• возраст;

• одноэтапное или многоэтапное голосование.

2. Свойства блока и вознаграждения. Выделяются для алгоритмов, заложенных в основу различных криптовалют. Эти свойства выражают преимущественно количественные характеристики, имеющие как прямое, так и косвенное влияние на достижение консенсуса в основанной на криптовалюте блокчейн системе, такие как:

a) дата создания первого блока;

b) общее предложение;

c) вознаграждение за создание блока;

d) среднее время создания блока.

3. Свойства безопасности. Содержат характеристики, описывающие сопротивляемость и защищённость сети от различных векторов атак:

a) наличие или отсутствие аутентификации;

b) устойчивость к цензуре;

c) соответствие стандартам неотказуемости;

d) вектор атаки.

4. Свойства производительности. Применяются для измерения количественных характеристик алгоритмов и включают следующие показатели:

a) максимально допустимое количество неисправных узлов;

b) число обрабатываемых за единицу времени транзакций;

c) масштабируемость без ухудшения показателей производительности;

d) задержка во времени между процессом согласования узлами предложения с транзакциями и моментом включения блока с транзакциями в общую цепочку;

е) энергопотребление.

Разновидности алгоритмов достижения консенсуса

Вне зависимости от логики алгоритмов консенсуса все они основаны на реализации основных правил взаимодействия пользователей, таких как достижение наибольшей степени согласия всех взаимодействующих сторон, соблюдение равноправия участников, заинтересованность участников в совместной работе и включение в процесс достижения консенсуса максимального числа участников [7]. Все механизмы консенсуса имеют следующие функции:

- генерация новых блоков записей с частотой, исключающей ситуации генерации каждым узлом своего и записываемого блоков;
- проверка хешей транзакций текущего и предыдущего блока и корректности подбора числа nonce для всех участников;
- определение вознаграждения в сети, обратно пропорционального её сложности;
- недопущение двойного списания средств.

Основные алгоритмы достижения консенсуса в распределённых системах имеют следующую логику [8]:

1. Proof of Work (POW). Основана на конкуренции всех узлов сети за вознаграждение при добавлении в конец цепочки блока записей. Выигравший узел, добавивший блок, получает вознаграждение цифровыми токенами.

2. Proof of Stake (POS). Предполагает, что пользователь, создающий новый блок, выбирается детерминированно в зависимости от его доли или богатства. Согласно данной концепции, вероятность успеха узла в создании новых токенов увеличивается пропорционально количеству уже принадлежащих узлу токенов.

3. Delegated Proof of Stake (DPOS). Используется для стимулирования заинтересованных сторон и их поощрения к участию в сети посредством делегирования либо передачи токенов более крупным заинтересованным сторонам.

4. Proof of Elapsed Time. Согласно этому согласованному механизму, все участвующие узлы должны идентифицировать себя перед участием в сети. Этот алгоритм основан на системе честной лотереи, где каждый участник обладает равными возможностями стать победителем.

5. Raft. Это отказоустойчивый алгоритм, следующий модели «лидера-последователя», при которой для принятия решения о состояниях сети и передаче изменений на узлы-последователи посредством случайных настроек тайм-аута избирается руководитель.

Первые три алгоритма являются наиболее распространёнными, однако при ряде обстоятельств подвержены взлому [9]. Так, в алгоритме POW участник может злоупотребить обществом союзников, способных в нужный момент сконцентрировать более 51 % компьютерной мощности, достигнув консенсуса в свою пользу. Алгоритм POS постепенно приводит к значительному разрыву в доходах, при котором с течением времени один либо группа участников могут сконцентрировать достаточные средства и влиять на достижение консенсуса не в интересах сообщества, а исключительно в личных интересах. Алгоритм DPOS является усовершенствованной версией POS, предполагающей решение свойственной ему проблемы явным делегированием права управления по назначению владеющими большими долями участниками, однако такой подход приводит только к ручному контролю над блокчейн системой.

Разработка новых алгоритмов консенсуса идёт по пути соответствия определённым требованиям, таким как: [10]

- время создания нового блока не более минуты;
- скорость поступления транзакций не менее 10^3 в секунду;
- количество участвующих в выработке консенсуса узлов 10^3-10^4;
- отсутствие значительных вычислительных мощностей и энергозатрат.

Удовлетворение указанным требованиям позволяет обеспечить высокую безопасность и производительность блокчейн системы.

Заключение

Алгоритмы достижения консенсуса блокчейн системы обеспечивают безопасность, живучесть и значительную пропускную способность сети и позволяют пользователям приходить к согласию касательно состояния транзакций на протяжении фиксированного количества шагов. Они обеспечивают надёжную работу системы даже в ненадёжных сетях, однако обладают определёнными недостатками, которые важно учитывать. Каждый из алгоритмов консенсуса реализует определённые логические зависимости, актуальность которых меняется в зависимости от ситуации, поэтому выбор логики алгоритмов консенсуса во многом зависит от конкретной задачи, имеющей уникальные характеристики.

Список литературы

1. Гумеров Э.А. Тенденции развития блокчейн систем // Образовательные ресурсы и технологии. – 2019. – № 2 (27). – С. 59-63.
2. Попадюк А.Ю., Коровяковский Е.К., Титова Т.С. Экологические аспекты технологии распределённого реестра на примере алгоритма консенсуса Proof-of-Work // Известия Петербургского университета путей сообщения. – 2020. – Т. 17, № 1. – С. 136-143.
3. Тороев А.С., Сизоненко А.Б. Алгоритм достижения консенсуса для распределённых систем обработки данных на основе технологии распределённых реестров // Моделирование, оптимизация и информационные технологии. – 2021. – № 9(1). – 9 с.
4. Жиленков А.А., Черный С.Г. Существование и достижимость консенсуса как проблема обеспечения надёжности в распределённых приложениях и киберфизических системах // Электротехнические и информационные комплексы и системы. – 2020. – № 2. – С. 92-104.
5. Носиров З.А., Фомичев В.М. Анализ блокчейн-технологии: основы архитектуры, примеры использования, перспективы развития, проблемы и недостатки // Системы управления, связи и безопасности. – 2021. – № 2. – С. 37-75.

6. Бахвалова Е.А., Судаков В.А. Исследование алгоритмов консенсуса для блокчейн-платформ // Препринты ИПМ им. М.В. Келдыша. – 2021. – № 26. – 16 с.
7. Бауэр В.П., Смирнов В.В. Институциональные особенности разработки конкурентоспособной криптовалюты. Финансы: теория и практика. – 2020. – № 24 (5). – С. 84-99.
8. Криштаносов В.Б. Блокчейн: технологический и экономический аспекты // Труды БГТУ. Серия 5: Экономика и управление. – 2020. – № 2 (238). – С. 13-32.
9. Колонин А. Репутационная система для онлайн-сообществ / А. Колонин, Б. Герцель, Д. Дуонг, М. Айкл, Н. Знидар // Агенты. – 2018. – 11 с.
10. Бардин А.П., Новицкий А.В., Шумилов Ю.Ю. Обработка ошибочных ситуаций в больших блокчейн-сетях алгоритмом достижения консенсуса, основанном на решении задачи византийских генералов // Вестник Московского государственного технического университета им. Н.Э. Баумана. Серия Приборостроение. – 2021. – № 4 (137). – С. 27-40.

Bibliography

1. Gumerov E.A. Trends in the development of blockchain systems // Educational resources and technologies. - 2019. - No. 2 (27). – S. 59-63.
2. Popadyuk A.Yu., Korovyakovsky E.K., Titova T.S. Ecological aspects of distributed ledger technology on the example of the Proof-of-Work consensus algorithm. Bulletin of the Petersburg University of Communications. - 2020. - T. 17, No. 1. - S. 136-143.
3. Toroev A.S., Sizonenko A.B. Algorithm for achieving consensus for distributed data processing systems based on distributed registry technology // Modeling, optimization and information technologies. - 2021. - No. 9(1). – 9 s.
4. Zhilenkov A.A., Cherny S.G. Existence and achievability of consensus as a problem of ensuring reliability in distributed applications and cyber-physical systems // Electrotechnical and information complexes and systems. - 2020. - No. 2. - P. 92-104.

5. Nosirov Z.A., Fomichev V.M. Blockchain technology analysis: fundamentals of architecture, examples of use, development prospects, problems and shortcomings // Control Systems, Communications and Security. - 2021. - No. 2. - P. 37-75.
6. Bakhvalova E.A., Sudakov V.A. Research of consensus algorithms for blockchain platforms // IPM preprints im. M.V. Keldysh. - 2021. - No. 26. - 16 p.
7. Bauer V.P., Smirnov V.V. Institutional features of the development of a competitive cryptocurrency. Finance: theory and practice. - 2020. - No. 24 (5). – S. 84-99.
8. Krishtanosov V.B. Blockchain: technological and economic aspects // Proceedings of BSTU. Series 5: Economics and Management. - 2020. - No. 2 (238). - S. 13-32.
9. Kolonin A. Reputation system for online communities / A. Kolonin, B. Herzel, D. Duong, M. Aikl, N. Znidar // Agents. - 2018. - 11 p.
10. Bardin A.P., Novitsky A.V., Shumilov Yu.Yu. Handling erroneous situations in large blockchain networks with a consensus algorithm based on solving the problem of Byzantine generals // Bulletin of the Moscow State Technical University. N.E. Bauman. Series Instrumentation. - 2021. - No. 4 (137). - S. 27-40.

© Чахкиев М.Т., 2022 Научно-образовательный журнал для студентов и преподавателей «StudNet» №3/2022

Для цитирования: Чахкиев М.Т. АЛГОРИТМЫ ДОСТИЖЕНИЯ КОНСЕНСУСА В БЛОКЧЕЙН СИСТЕМЕ// Научно-образовательный журнал для студентов и преподавателей «StudNet» №3/2022