Маркова Т.Д. Масштабируемость блокчейн сетей // Международный журнал информационных технологий и энергоэффективности.– 2024. –Т. 9 № 11(49) с. 68–73

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.942.2

МАСШТАБИРУЕМОСТЬ БЛОКЧЕЙН СЕТЕЙ

Маркова Т.Д.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: norm_staffchik@mail.ru

Технология блокчейна, обеспечивающая децентрализованный, безопасный и прозрачный учет данных, сталкивается с серьезными проблемами масштабируемости, которые ограничивают ее применение в приложениях, требующих высокой пропускной способности. В настоящей статье анализируются ключевые ограничения масштабируемости существующих блокчейн-сетей, такие как ограниченная пропускная способность, высокая стоимость транзакций, высокая задержка подтверждения транзакций и небольшое количество транзакций в блоке. Рассматриваются фундаментальные причины этих проблем, включая распределенный консенсус, необходимость избыточности данных, ограничения вычислительных мощностей и трудоемкость майнинга. Основное внимание уделяется перспективным решениям для повышения масштабируемости на различных уровнях: блокчейна, сети, консенсуса и криптографии. Анализируются такие решения, как увеличение размера блока, шардинг, каналы состояния, сети ретрансляции, альтернативные алгоритмы консенсуса и новые криптографические доказательства. Проводится сравнительный анализ применения этих решений и их комбинаций на ведущих блокчейн-платформах, включая Bitcoin, Ethereum, EOS и другие. В заключение обсуждаются компромиссы и перспективы дальнейшего развития масштабируемых блокчейн-решений.

Ключевые слова: Блокчейн, масштабируемость, пропускная способность, шардинг, консенсус, криптография, каналы состояния, Bitcoin, Ethereum, EOS.

SCALABILITY OF BLOCKCHAIN NETWORKS

Markva T.D.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: norm_staffchik@mail.ru

Blockchain technology, which provides decentralized, secure and transparent data accounting, faces serious scalability problems that limit its use in applications requiring high bandwidth. This article analyzes the key scalability limitations of existing blockchain networks, such as limited bandwidth, high transaction costs, high transaction confirmation latency, and a small number of transactions per block. The fundamental causes of these problems are considered, including distributed consensus, the need for data redundancy, limitations of computing power and the complexity of mining. The focus is on promising solutions to increase scalability at various levels: blockchain, network, consensus, and cryptography. Solutions such as block size increase, sharding, state channels, relay networks, alternative consensus algorithms and new cryptographic proofs are analyzed. A comparative analysis of the application of these solutions and their combinations on leading blockchain platforms, including Bitcoin, Ethereum, EOS and others, is carried out. In conclusion, the trade-offs and prospects for further development of scalable blockchain solutions are discussed.

Keywords: Blockchain, scalability, bandwidth, sharding, consensus, cryptography, fortune channels, Bitcoin, Ethereum, EOS.

Революционная технология блокчейна открыла новую эру децентрализованных систем, обеспечивающих беспрецедентный уровень безопасности, надежности и прозрачности

записей данных. Блокчейн представляет собой распределенную базу данных, состоящую из цепочки блоков, которые криптографически связаны и распределены по множеству узлов в одноранговой сети. Эта инновационная архитектура устраняет необходимость в централизованном управлении, позволяя участникам сети совершать безопасные транзакции и хранить неизменяемую историю записей без вмешательства третьей стороны.

Принцип работы блокчейна основан на использовании криптографических хеш-функций, асимметричного шифрования и алгоритмов консенсуса. Когда новая транзакция вводится в сеть, она должна быть проверена и подтверждена большинством участников (майнеров) в соответствии с установленными правилами консенсуса. После подтверждения транзакция записывается в новый блок данных, который криптографически связывается с предыдущим блоком, формируя неразрывную цепочку блоков или блокчейн. Эта архитектура гарантирует, что записанные данные не могут быть изменены или удалены без нарушения всей последовательности блоков.

Одним из ключевых преимуществ блокчейн-технологии является ее децентрализованная природа, которая исключает единую точку отказа и уязвимость к атакам или сбоям. Кроме того, блокчейн обеспечивает высокий уровень безопасности и неизменности данных благодаря использованию криптографических алгоритмов и принципа распределенного реестра. Транзакции в блокчейне полностью прозрачны и могут быть проверены любым участником сети, что повышает доверие и подотчетность системы.

Несмотря на многочисленные преимущества, одной из основных проблем, сдерживающих массовое внедрение технологии блокчейна, является ограниченная масштабируемость существующих блокчейн-сетей. Из-за консенсусного механизма валидации транзакций и распределенной природы блокчейна возникают ограничения по пропускной способности, времени подтверждения транзакций и стоимости обработки. Эти факторы препятствуют использованию блокчейна в приложениях, требующих высокой пропускной способности и низкой задержки, таких как платежные системы, игры, социальные сети и многие другие.

В данной статье мы рассмотрим текущие проблемы масштабируемости блокчейн-сетей, проанализируем их основные причины и исследуем перспективные решения, предлагаемые исследователями и разработчиками для преодоления этих ограничений. Мы также сравним различные подходы и оценим их эффективность и применимость для различных блокчейн-платформ.

Несмотря на многочисленные преимущества технологии блокчейна, существующие блокчейн-сети сталкиваются с серьезными проблемами масштабируемости, которые значительно ограничивают их возможности и применимость в различных областях. Рассмотрим основные ограничения масштабируемости подробнее:

1. Ограниченная пропускная способность

Пропускная способность блокчейна определяется количеством транзакций, которые могут быть обработаны и подтверждены в единицу времени. В большинстве популярных блокчейн-сетей, таких как Bitcoin и Ethereum, пропускная способность сильно ограничена. Например, в сети Bitcoin может быть обработано только около 7 транзакций в секунду, а в Ethereum - около 15 транзакций в секунду. Эти показатели значительно ниже, чем у традиционных централизованных систем платежей, которые обрабатывают тысячи транзакций в секунду.

2. Высокая стоимость транзакций

В блокчейн-сетях майнеры получают вознаграждение за валидацию и включение транзакций в блоки. Однако из-за ограниченной пропускной способности и растущей популярности блокчейнов, стоимость комиссий за транзакции может быть очень высокой, особенно в периоды высокой нагрузки на сеть. Это делает некоторые приложения на базе блокчейна экономически невыгодными для пользователей.[1]

3. Высокая задержка подтверждения транзакций

Время, необходимое для подтверждения транзакции в блокчейне, зависит от времени генерации нового блока и количества подтверждений от майнеров. В Bitcoin новый блок генерируется примерно каждые 10 минут, а для надежного подтверждения транзакции требуется от 6 до 10 подтверждений, что может занять около часа. Такая высокая задержка неприемлема для многих приложений, требующих быстрых транзакций, таких как платежные системы или игры.

4. Ограниченное количество транзакций в блоке

Размер блока в блокчейне обычно ограничен для обеспечения эффективной распространяемости блоков по сети. Например, в Bitcoin размер блока ограничен 1 МБ, что позволяет обрабатывать только около 2000-3000 транзакций в каждом блоке. Это ограничение также накладывает пределы на общую пропускную способность системы.

Эти фундаментальные ограничения масштабируемости являются серьезными препятствиями для широкого внедрения технологии блокчейна в различных областях, требующих высокой производительности, низкой задержки и низких комиссий за транзакции. В следующих разделах мы рассмотрим причины этих ограничений и возможные решения для повышения масштабируемости блокчейн-сетей.

Далее речь пойдет о причинах проблем масштабируемости.

В блокчейн-сетях все узлы должны достичь консенсуса относительно текущего состояния распределенного реестра. Этот процесс требует значительных вычислительных ресурсов и времени, так как каждый узел должен проверить и подтвердить каждую транзакцию. Чем больше узлов в сети, тем сложнее достичь консенсуса, что ограничивает общую пропускную способность.

Для обеспечения децентрализации и устойчивости к сбоям, каждый узел в блокчейн-сети должен хранить полную копию распределенного реестра. Это требует значительных затрат ресурсов по мере роста размера блокчейна, что ограничивает масштабируемость.[2]

Многие алгоритмы консенсуса, такие как Proof-of-Work, требуют интенсивных вычислений для решения криптографических задач. Эти вычисления ограничивают скорость генерации новых блоков и, следовательно, пропускную способность сети.

В блокчейнах с Proof-of-Work майнинг новых блоков требует значительных вычислительных ресурсов и энергозатрат. По мере роста сложности майнинга и централизации вычислительных мощностей, процесс валидации транзакций замедляется, снижая общую пропускную способность.[3]

Ниже рассмотрим перспективные решения на разных уровнях.

На уровне блокчейна можно применить следующие действия:

- Увеличение размера блока - позволяет включать больше транзакций в каждый блок, но требует больших ресурсов для передачи и хранения.
- Сегрегированные адресные индексы - оптимизация данных для уменьшения объема блокчейна.

- Блокчейн-шардинг - горизонтальное масштабирование блокчейна путем разделения на несколько параллельных цепочек (шардов).[4]

На уровне сети можно попробовать такие способы:

- Отложенные транзакции и каналы состояния - выполнение транзакций вне основной цепи с периодическими фиксациями в блокчейне.
- Сети ретрансляторов транзакций - распределение транзакций за пределами основной сети для повышения пропускной способности.

На уровне консенсуса - алгоритмы консенсуса без майнинга (PoS, DPoS и др.) - более энергоэффективные альтернативы Proof-of-Work.

Что касается уровня криптографии, тут можно использовать овые типы криптографических доказательств (zk-SNARKs, Bulletproofs и др.) - позволяют верифицировать транзакции без раскрытия всех данных, уменьшая нагрузку на сеть.

Сравнительный анализ предложенных решений и их комбинаций на разных блокчейн-платформах:

Bitcoin

- Увеличение размера блока (Bitcoin Cash, Bitcoin SV)
- Сегрегированные адреса (Segregated Witness в Bitcoin)
- Каналы состояния (Lightning Network)
- Блокчейн-шардинг пока не реализован

Ethereum

- Увеличение газового лимита в блоке (временное решение)
- Шардинг планируется в обновлении Ethereum 2.0
- Каналы состояния (Raiden Network, Perun)
- Rollups (Optimistic и ZK-rollups) для выноса данных за пределы основной цепи
- Переход на Proof-of-Stake в Ethereum 2.0

EOS

- Горизонтальное масштабирование через параллельные цепочки (sharding)
- Делегированный алгоритм консенсуса Proof-of-Stake (DPoS)
- Параллельная обработка транзакций
- Отсутствие комиссий за транзакции

Комбинация различных решений часто является наиболее эффективной стратегией. Например, в Ethereum 2.0 планируется использовать шардинг цепи, rollup-технологии, PoS и другие оптимизации одновременно.

При выборе решения следует учитывать специфику платформы, требования приложения, готовность к компромиссам. Основные компромиссы лежат в плоскости децентрализации, безопасности, и универсальности. Например, шардинг повышает производительность, но снижает степень децентрализации. А оптимистические rollup-решения ускоряют транзакции, но требуют доверия к оператору.

В целом, блокчейн индустрия движется в сторону многоуровневых решений, совмещающих различные подходы на разных уровнях стека. Ведущие платформы активно экспериментируют и развивают множество перспективных методов наряду с оптимизацией базовой архитектуры блокчейна.

Проблема масштабируемости является одним из ключевых вызовов, стоящих на пути широкого внедрения технологии блокчейна. В настоящей работе мы проанализировали

основные ограничения масштабируемости существующих блокчейн-сетей и рассмотрели перспективные решения, предлагаемые для преодоления этих ограничений на разных уровнях.[5]

Хотя многие из описанных решений, такие как увеличение размера блока, шардинг, каналы состояния и новые криптографические доказательства, демонстрируют многообещающие результаты в повышении масштабируемости, ни одно из них не является идеальным и универсальным. Каждое решение имеет свои компромиссы и ограничения в плане децентрализации, безопасности, универсальности или требует значительных архитектурных изменений.

По мере дальнейшего развития блокчейн-технологий и ее применения в различных областях, наиболее эффективным подходом, вероятно, станет комбинирование нескольких решений на разных уровнях стека. Уже сейчас ведущие блокчейн-платформы активно экспериментируют с многоуровневыми архитектурами, совмещающими шардинг, каналы состояния, rollup-технологии, новые алгоритмы консенсуса и другие инновации.

Кроме того, важно отметить, что повышение масштабируемости не является единственной задачей. Разработчики блокчейн-решений должны также учитывать такие аспекты, как децентрализация, безопасность, устойчивость к цензуре и конфиденциальность данных. Достижение оптимального баланса между этими факторами будет ключевым для успешного массового внедрения блокчейн-технологий.

В целом, исследования в области масштабируемости блокчейнов активно продолжаются, и можно ожидать появления новых перспективных решений в ближайшем будущем. Междисциплинарное сотрудничество между криптографами, разработчиками консенсусных алгоритмов, специалистами по распределенным системам и другими экспертами будет иметь решающее значение для достижения прогресса в этой области.

Список литературы

1. Виткова Л. А., Ахрамеева К. А., Грузинский Б. А. Использование геометрических хеш-функций в информационной безопасности //Известия высших учебных заведений. Технология легкой промышленности. – 2017. – Т. 37. – №. 3. – С. 5-9.
2. Небаева К. А. Разработка необнаруживаемых стегосистем для каналов с шумом //СПб.: СПбГУТ. – 2014. – Т. 176.
3. Ахрамеева К. А. и др. Анализ средств обмена скрытыми данными злоумышленниками в сети интернет посредством методов стеганографии //Телекоммуникации. – 2020. – №. 8. – С. 14-20.
4. Березина Е. О., Виткова Л. А., Ахрамеева К. А. Классификация угроз информационной безопасности в сетях IOT //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2020. – №. 2. – С. 11-18.
5. Бирих Э. В., Ферапонтова С. С. К вопросу об аудите персональных данных //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). – 2018. – С. 111-114.

References

1. Tsvetkova L. A., Akhrameeva K. A., Gruzinsky B. A. The use of geometric hash functions in information security //News of higher educational institutions. Light industry technology. - 2017. – Vol. 37. – No. 3. – pp. 5-9.
2. Nebaeva K. A. Development of undetectable stegosystems for channels with noise //St. Petersburg: SPbSUT. – 2014. – Vol. 176.
3. Akhrameeva K. A. et al. Analysis of the means of exchanging hidden data by intruders on the Internet using steganography methods //Telecommunications. - 2020. – No. 8. – pp. 14-20.
4. Berezina E. O., Vitkova L. A., Akhrameeva K. A. Classification of information security threats in IOT networks //Bulletin of the St. Petersburg State University of Technology and Design. Series 1: Natural and Technical Sciences. – 2020. – No. 2. – pp. 11-18.
5. Birikh E. V., Ferapontova S. S. On the issue of personal data audit //Actual problems of infotelecommunications in science and education (APINO 2018). – 2018. – pp. 111-114.