Эффективный алгоритм консенсуса блокчейн сети

Горелышев Сергей Станиславович

аспирант

Московский авиационный институт (национальный исследовательский университет), Москва, Россия

E-mail: gorelushev.sergey@yandex.ru

Научный руководитель *— Зайцев Валентин Евгеньевич*

В настоящее время все большее распространение получают распределенные системы вычисления, облачные технологии и децентрализованное хранение данных. Однако, при всех их преимуществах возникают и новые проблемы. В основном они касаются защищённости данных, циркулирующих в распределенной сети, их целостности и конфиденциальности. Кроме того, при существенном увеличении объёма распределённых данных возникают сложности с масштабированием сети и с обеспечением необходимой скорости обработки данных блокчейна [1,2]. Хотя технология блокчейн развивается как обособленная, она может использоваться и за рамками систем криптовалют. Применение данной технологии в различных областях цифровой экономики и бизнеса становится все более перспективным. Преимущества и недостатки технологии блокчейна хорошо известны [1,2,3,4], в частности обращается внимание на недостаточную исследованность таких аспектов применения блокчейна, как безопасность, достоверность данных, быстродействие, эффективность протокола взаимодействия узлов (выработка консенсуса) в сети блокчейн. Существуют тысячи различных блокчейн сетей, которые являются либо публичными (открытый код) либо частными, Наиболее популярными и быстрыми блокчейнами являются: Bitcoin со скоростью 7–10 транзакций в секунду (TPS), Ethereum (15–30 TPS), Minter (2000 TPS), Cardano (5000 TPS), QTUM (10000 TPS), Solana (50000 TPS), Everscale (68000 TPS) и др. Анализ функционирования вышеперечисленных современных блокчейнов и их характеристик показал, что повышение скорости обработки и финализации транзакций сетью (масштабируемость) блокчейна достигается либо децентрализацией, либо снижением безопасности. Для решения данной проблемы необходима такая организация функционирования блокчейна, которая обеспечит как ее безопасное устройство, так и ограничение нагрузки на узлы системы.

Одним из методов решения проблемы масштабирования являет-

ся использование направленных ациклических графов. Однако, данный метод не является блокчейном в чистом виде, так как передача данных происходит без доказательства корректности работы валидаторов [3]. Не меньшим потенциалом повышения производительность блокчейна обладает сегментация сети (шардинг). Такой подход позволяет разделить сеть на несколько более управляемых сегментов, что дает возможность масштабировать сеть и увеличить ее пропускную способность. Сама идея шардинга заключается в том, чтобы исполнение транзакций распределить между различными сегментами (шардами), и чтобы каждый шард выступал в роли маленького блокчейна. Как показала практика, данный подход дает возможное решение проблемы масштабирования сети. Однако, коммуникация и безопасность (стандартная атака «51%») остаются главными проблемами шардинга. Важным аспектом развития технологии блокчейна является усовершенствование алгоритма консенсуса, который позволит оптимизировать работу и повысить защищенность сети блокчейн, особенно с технологией шардинга. Одни алгоритмы позволяют строить защищённые децентрализованные системы, другие — с большой пропускной способностью и масштабируемостью [4]. Основные алгоритмы консенсуса: Proof-of-Work (PoW) — вклад валидатора определяется затратами на вычисление; Proof-of-Stake (PoS) — вклад валидатора зависит от доли внесенных денежных единиц; Delegated Proof-of-Stake (DPoS), Thresholded Proof-of-Stake (TPoS) — разновидности PoS, использующие принципы представительной демократии; Byzantine Fault Tolerance (BFT) — направленные на коллективное принятия решения и уменьшение влияния неисправных узлов.

Сравнение основных алгоритмов консенсуса приведено в табл. 1.

В последнее время расширение практического применения блокчейна приводит к тому, что всё больше проектов отходят от PoW и переходят к альтернативным алгоритмам консенсуса. Автором выполнено построение и реализация эффективной модели осуществления консенсуса узлов с учетом шардинга, а также разработка оптимизированного алгоритма консенсуса, учитывающего аспекты безопасности, сетевой нагрузки и времени договоренности между узлами сети. Предлагается комбинированный PoS–BFT алгоритм консенсуса с шардингом данных и валидаторов сети, с ротацией валидаторов в различных сегментах блокчейна (шардах) для сохранения необходимого уровня безопасности масштабируемой сети. Производительность алгоритма в TPS показывает достижение необходимой масштабируемости сети, а наличие шардинга даёт возможность

практически неограниченного роста быстродействия сети при увеличении количества валидаторов.

Таблица 1 – Характеристики основных алгоритмов консенсуса

Алгоритмы	Примеры проектов	Энергозатраты, кВт*ч/день	Количество узлов	Управление	Приоритетные характеристики
PoW	Bitcoin Ethereum	69974983/ 51765837	10102/ 12754	оффчейн-управление	децентрализованность, безопасность
PoS	Cardano	18630	12	ончейн-управление	масштабируемость
DPoS	Minter	30-45	16-256	ончейн-голосование	масштабируемость, низкое энергопотребление
TPoS	Near	—	—	ончейн-голосование	масштабируемость
BFT	Neo	51	7	ончейн-голосование, оффчейн управление	масштабируемость, низкое энергопотребление

При этом проблема сохранения безопасности сети требует дополнительного экспериментального исследования. Теоретическая оценка вероятности захвата одной шарды получена. Прототип алгоритма в реальных условиях подтверждает ожидаемую эффективность, превосходя стандартные алгоритмы консенсуса.

Литература

1. Цветкова Л. А. Перспективы развития технологии блокчейн в России: конкурентные преимущества и барьеры. Экономика науки: –М., РАНХиГС, 2017. Т. 3, № 4. С. 275–296. ISSN 2410–132X.
2. Пряников М. М., Чугунов А. В. Блокчейн как коммуникационная основа формирования цифровой экономики: преимущества и проблемы. Internetional Journal of Open Information Technologies. 2017. Т. 5, № 6. С. 49–55.
3. Утавкаева И. Х., Никитенко В. О., Тутаев И. А. Особенности внедрения технологии блокчейн в цифровую экономику. Вестник алтайской академии экономики и права. 2019. № 7. С. 91–95.
4. Равал С. Децентрализованные приложения. Технология Blockchain в действии. СПб.: Питер, 2017.