УДК 004.77

ПОНЯТИЕ ТЕХНОЛОГИИ БЛОКЧЕЙН

К.С. ГОЛОВАН
(Представлено: канд. физ.-мат. наук, доц. О.В. ГОЛУБЕВА)

Раскрываются понятия блокчейна, децентрализованной сети, разрешения консенсуса, приватного и публичного блокчейна. Приводятся примеры современных блокчейн-решений. Блокчейн позволяет безопасно распространять и/или обрабатывать данные между несколькими лицами через недоверенную сеть. Наиболее интересным вариантом данных является возможность передачи информации, которая требует наличия третьей доверенной стороны.

Блокчейн – это журнал с фактами, реплицируемый на несколько компьютеров, объединенных в сеть равноправных узлов (P2P). Фактами может быть что угодно – от денежных операций и до подписания контента. Члены сети – анонимные лица, называемые узлами. Все коммуникации внутри сети используют криптографию, чтобы надежно идентифицировать отправителя и получателя. Когда узел стремиться добавить факт в журнал, в сети формируется консенсус, чтобы определить, где этот факт должен появиться в журнале; этот консенсус называется блоком.

Децентрализованные сети с равноправными узлами появились задолго до блокчейна. К примеру, BitTorrent, только вместо обмена файлами в блокчейне обмениваются фактами.

P2P-сетям, как и прочим распределенным системам, приходится решать сложную проблему информатики – разрешение конфликтов, или согласование. Реляционные базы данных предлагают ссылочную целостность, но такой особенности нет в распределенной системе. Если два несовместимых факта прибывают в одно и то же время, система должна иметь правила для определения того, какой факт считать правильным.

В P2P сетях, два факта отправленные примерно в одно время могут прибыть в разном порядке в удаленные узлы. Тогда, каким образом всей сети согласовать, какой факт пришел первым?

Чтобы гарантировать целостность в P2P сети, вам нужен способ согласования порядка фактов. Вам нужна система консенсуса.

Алгоритмы консенсуса для распределенных систем это очень активное поле для исследований [1].

Задача распределенного консенсуса не специфична для блокчейнов и имеет хорошо проверенные решения для многих других распределенных систем (например, баз данных NoSQL). Но биткойн и другие блокчейны от предыдущих наработок отличаются условиями работы сети.

В обычных алгоритмах византийского консенсуса у узлов сети есть «личности», выражаемые через цифровые подписи или сходные криптопримитивы, а сам список узлов известен заранее или меняется редко, но предсказуемо. В биткойн-блокчейне все наоборот.

Участники сети не только заранее неизвестны, но и могут свободно подключаться или отключаться от сети. При этом блокчейн, являясь децентрализованной системой, имеет определенные свойства: устойчивость к цензуре (никто не может запретить майнить криптовалюту) и объективность (для определения текущей версии журнала транзакций не нужно доверие неким авторитетным источникам – корень доверия находится в самом блокчейне).

Из-за этого обычные алгоритмы византийского консенсуса для блокчейна не подходят. Поэтому было предложено множество различных алгоритмов, среди которых выделяются две основные категории: алгоритмы на основе доказательства работы (proof-of-work) и алгоритмы на основе подтверждения доли (proof-of-stake).

В случае доказательства работы хеш сообщения, объединенного со специальным полем (nonce), должен быть меньше определенного значения (или начинаться с определенного числа нулевых битов). Nonce не несет смысла для самого сообщения – это поле перебирается автором доказательства, пока не будет найдено подходящее значение. Название «доказательство работы» отражает тот факт, что для нахождения nonce надо совершить вычислительную работу, ожидаемое количество которой измеримо. Например, если нужно, чтобы первые 16 бит хеша равнялись нулю, в среднем нужно перебрать 65 536 значений nonce.

Доказательство работы похоже на цифровые подписи – оно обеспечивает целостность сообщения, так как вероятность того, что один и тот же nonce подойдет для различных сообщений, очень мала. Доказательства также легко проверяются – достаточно провести лишь одну операцию хеширования. В отличие от подписей, создание доказательства работы не требует знания секретов, но «потребляет» больше вычислительных ресурсов. Доказательства работы используются узлами биткойна для определения состояния системы. Актуальный журнал транзакций определяется как цепочка блоков с наибольшей сум-

марной сложностью доказательств работы. Майнеры, соответственно, должны искать блок поверх этой цепочки. Но, теоретически, никто не запрещает создавать новые блоки на основе какого-то старого блока (иногда случаются расщепления – форки – блокчейна, потому что два майнера находят новый блок практически одновременно). Однако намеренные форки невыгодны экономически, потому что блоки из побочных ветвей блокчейна никем не учитываются и не приносят их создателям никакой прибыли – одни затраты на нахождение доказательства работы.

Консенсус Накамото обеспечивает два ключевых требования к блокчейну, которые мы выделили ранее. Из-за того, что доказательство работы не привязывается к личностям майнеров (в отличие от цифровых подписей/сертификатов), обеспечивается устойчивость к цензуре. А за счет того, что доказательства работы быстро проверяются и не требуют для проверки ничего, кроме блокчейна, достигается объективность протокола.

Консенсус Накамото устойчив к атакам на сеть блокчейна, причем его безопасность достаточно хорошо исследована теоретически (в отличие от более новых предложений для блокчейнов). В оригинальной статье отмечено, что сеть биткойна продолжит адекватно функционировать, даже если половина майнеров начнет злонамеренную активность. Если же среди майнеров появится злонамеренное большинство (так называемая атака 51%), они смогут игнорировать блоки от всех остальных майнеров, чтобы забрать себе всю награду в сети, или, например, мошенничать, производя повторную трату средств за счет намеренных форков блокчейна. Однако при этом отметим, даже если все майнеры в сети сговорятся, они не смогут обойти базовые механизмы безопасности биткойна – например, не смогут похитить биткойны пользователей.

У консенсуса Накамото есть свойство, которое многими воспринимается как большой недостаток – для обеспечения безопасности нужно «работать», то есть производить доказательства работы. Вычисления, которые выполняются в рамках PoW, не служат никакой полезной цели, и это архитектурная особенность. Оказывается, очень сложно придумать доказательство работы, которое бы выполняло общественно полезную роль. Поэтому может показаться, что ресурсы (прежде всего, электричество) на майнинг тратятся впустую (если не считать, что они тратятся на обеспечение безопасности).

Помимо этого, майнинг все же подвержен проблеме централизации. Более 70% хешрейта биткоина на данный момент находится в одной стране – Китае. Многие криптовалюты пытаются децентрализовать майнинг за счет использования доказательств работы, которые экономически невыгодно вычислять на специализированном оборудовании, однако с таким подходом возникает другая проблема – если сделать выгодным майнинг биткоинов с помощью домашних компьютеров, то арендовать оборудование для атаки (или создать для нее ботнет) станет существенно дешевле и проще.

Пытаясь решить эти проблемы, сообщество предлагает множество алгоритмов консенсуса, которые не требуют «работы». Самая популярная категория таких алгоритмов основана на доказательствах доли (proof-of-stake, PoS). Доказательство доли похоже на доказательство работы, только вместо совершения определенной работы автор показывает, что у него есть доля в системе (например, в виде ненулевого баланса криптовалюты).

Однако у доказательства доли есть досадный недостаток в сравнении с PoW: поскольку доказательства доли базируются не на реальном мире (вычислительная мощность), а на чем-то внутри самого блокчейна (баланс криптовалюты), задача построения надежного PoS-алгоритма оказывается нетривиальной [3].

Согласно последним исследованиям в области блокчейнов компании BitFury, выделяются следующие типы блокчейнов:

Открытый блокчейн (англ. publicblockchain) – блокчейн, в котором не существует ограничений на чтение данных блоков (при этом данные могут быть зашифрованы) и ограничений на отсылку транзакций для включения в блокчейн.

Закрытый блокчейн (англ. privateblockchain) – блокчейн, в котором прямой доступ к данным и отправке транзакций ограничен определенным узким кругом организаций.

Общедоступный (инклюзивный) блокчейн (англ. permissionlessblockchain) – блокчейн, в котором не существует ограничений на личность обработчиков транзакций (т.е. пользователей, которые могут создавать блоки транзакций).

Эксклюзивный блокчейн (англ. permissionedblockchain) – блокчейн, в котором обработка транзакций осуществляется определенным списком субъектов с установленными личностями.

Приватные блокчейны имеют определенные преимущества: *во-первых*, низкая стоимость транзакций, поскольку проверка их валидности проводится доверенными и высокопроизводительными узлами вместо десятков тысяч пользовательских устройств, как в случае с общедоступными сетями; *во-вторых*, блокчейн можно настроить таким образом, что показатель TPS (TPS – transactionspersecond) будет значительно большим, чем у общедоступных сетей (по крайней мере, в ближайшем будущем). Единственным ограничением в этом случае остается пропускная способность самого слабого узла в сети.

Еще одним преимуществом приватных блокчейнов может являться больший контроль над системой со стороны компании. Суть в том, что приватный блокчейн позволяет, например, быстро обновлять функциональность. Поэтому он привлекателен для учреждений, работающих с реестрами и системами учета, поскольку формирует контролируемую и прогнозируемую среду, по сравнению с общедоступными блокчейнами (о которых речь пойдет ниже).

Более того, создание блоков в приватном блокчейне зачастую не требует «доказательства работы» (proof-of-work). В качестве примера можно привести протокол создания блоков, используемый в BitShares. Имеется установленное число обработчиков транзакций *N*, каждый из которых обладает парой ключей – секретным и открытым. Создатели блоков известны и определяются по цифровой подписи в заголовке.

Операторы формируют блоки по очереди через заданные временные интервалы. Порядок создания блоков или фиксирован, или перемешивается после полного цикла (*N* блоков). Если оператор не сумел сформировать блок в отведенное ему время, то он пропускает раунд. Если такое поведение стало результатом злоумышленников, то ситуация расследуется. Таким образом, если обработчики транзакций являются единственными потребителями данных блокчейна, можно построить надежный протокол создания блоков (например, немного усложнив приведенный выше алгоритм), который не будет использовать доказательство работы.

И хотя приватные блокчейны могут и не использовать доказательство работы, этот протокол все-таки может быть подключен для повышения уровня защищенности, упрощения аудита и, как результат, повышения контроля над системой для конечных пользователей. По сути, доказательство работы переводит доверие к блокчейну из субъективного (доверие к системе эквивалентно доверию к контролирующей его организации) к объективному (доверие к системе вытекает из математических законов и гарантированно высокой экономической стоимостью атаки на систему, которая не зависит от личности атакующего).

Публичные или общедоступные блокчейны могут быть прочитаны любым пользователем, каждый из которых имеет право формировать транзакции. При этом операции защищаются механизмами криптографической верификации, такими как доказательство выполнения работы или подтверждение доли (proof-of-stake).

«Контролирует» публичный блокчейн сразу все сообщество участников сети – разработчики, пользователи, поставщики услуг, майнеры – которые обеспечивают целостность сети и удобство работы в ней. Эффективность работы сети достигается с помощью обновлений протокола, предотвращающих вредные изменения. Именно поэтому система позволяет создавать децентрализованные приложения с минимумом затрат на техническое обслуживание.

Также они предоставляют способ защиты пользователей приложения от разработчиков, ограничивая возможности последних. В приложениях на публичном блокчейне разработчик не может сам по себе изменять код или данные.

Помимо этого, публичные блокчейны обладают сетевыми эффектами. Первыми пользователями приложений, построенных на публичном блокчейне, зачастую являются пользователи других приложений на том же блокчейне, которые узнали о них благодаря эффекту взаимодействия программ. Например, мобильный кошелек, работающий на публичном блокчейне, может добавить функцию для взаимодействия этого приложения с другими распределенными приложениями на этом же блокчейне, значительно расширив свою пользовательскую базу.

Стоит отметить, что публичные блокчейны позволяют разрешить проблему передачи «товаров». Например, если пользователь *A* хочет продать домен пользователю *B*, то они сталкиваются с определенными трудностями. Если *A* передаст домен первым, то рискует не получить деньги, в ином случае *B* рискует не получить «товар». Для решения этой проблемы применяются посредники, взимающие проценты за проведение транзакции.

Однако если блокчейн имеет систему доменных имен и валюту, расходы сокращаются до нуля с использованием смарт-контракта. Первый отправляет программе домен, а второй – деньги. Проблем не возникает, поскольку программа является доверенной, так как действует в публичном блокчейне [2].

Заключение

Блокчейн позволяет безопасно распространять и/или обрабатывать данные между несколькими лицами через недоверенную сеть. Данными может быть что угодно, но наиболее интересным вариантом данных является возможность передачи информации, которая требует наличия третьей доверенной стороны. Примерами такой информации являются деньги (требуют участия банка), права на собственность (требуют участия нотариуса), договор на заем и т.д. В сущности, блокчейн устраняет необходимость в участии третьего доверенного лица.

С технической точки зрения блокчейн является новшеством, которое опирается на три понятия: P2P сети, асимметричная криптография и распределенный консенсус, основанный на решении математической задачи.

Блокчейн можно рассматривать как слабоинхронизированную базу данных, реплицируемую столько же раз, сколько узлов в сети, или как суперкомпьютер, образованный комплексом всех CPU/GPU входящих в него узлов.

Одно из главных преимуществ блокчейнов по сравнению с другими моделями распределенных баз данных – интеграция обработки информации, слежения за корректностью и безопасности в единый протокол, минимизирующий влияние человеческого фактора. Из-за юридических и технических причин учреждения, в которых задействованы финансовые системы учета или реестры, в среднесрочной перспективе могут быть заинтересованы в использовании блокчейнов с ограниченным доступом к обработке транзакций.

Что касается публичных блокчейнов, то их преимущества (в частности, их прозрачность и открытость базовых технологий и протоколов) могут привести к тому, что технология заменит многие функции традиционных финансовых институтов, изменив принципы работы финансовой системы

ЛИТЕРАТУРА

1. Объяснение блокчейна для веб-разработчиков [Электронный ресурс] / Ч. 1 : Теория. – Франция, 2016. – Режим доступа: https://marmelab.com/blog/2016/04/28/blockchain-for-web-developers-the-theory.html. – Дата доступа: 30.09.2017.
2. Различия, достоинства, недостатки: публичные и приватные блокчейны [Электронный ресурс]. – Россия, 2016. – Режим доступа: https://habrahabr.ru/company/bitfury/blog/324458/. – Дата доступа: 30.09.2017.
3. «Алгоритмы консенсуса»: Подтверждение доли и доказательство работы [Электронный ресурс]. – Россия, 2016. – Режим доступа: https://habrahabr.ru/company/bitfury/blog/327468/. – Дата доступа: 30.09.2017.