"Атака 51%" и устойчивость блокчейна биткоина

Александр Подобных, *руководитель Санкт-Петербургского РО АРСИБ, руководитель Комитета по безопасности цифровых активов и противодействию мошенничеству, судебный эксперт*

Децентрализованная сеть биткоина ставит метки времени на транзакции, соединяя их в цепочку доказательств проделанной работы на основе хеширования. Сформированные таким образом записи невозможно изменить, не выполнив заново всего объема вычислений. Самая длинная версия цепочки служит не только подтверждением очередности событий, но и доказывает, что над ней произвел работу самый большой вычислительный сегмент сети. Система находится в безопасности, пока под совокупным контролем ее честных участников находится больше вычислительной мощности, чем под контролем группы действующих совместно злоумышленников. В противном случае реализуется сценарий, названный “атака 51%”.

До тех пор пока большая часть вычислительных мощностей контролируется узлами, не объединенными с целью атаковать сеть, они будут генерировать самую длинную цепочку, опережая любых злоумышленников. Устройство самой сети очень простое: сообщения рассылаются на основе принципа наименьших затрат, а узлы могут покидать сеть и снова подключаться к ней в любой момент, принимая самую длинную версию цепочки для восстановления пропущенной истории транзакций.

Технологическая устойчивость биткоина основана на криптографии, а не на доверии третьей стороне, как это происходит в традиционных финансах. Вычислительная сложность и, как следствие, дороговизна отмены транзакций ограждает продавцов от мошенничества.

Доказательство работы

Для реализации распределенного одноранговой сервера меток времени разработчики использовали схему "доказательство работы", подобную системе Hashcash. Ее суть заключается в поиске такого значения, хеш которого (например, SHA-256) начинался бы с некоторого числа нулевых битов. Требуется выполнить объем работы, экспоненциально зависящий от числа нулей, но для проверки найденного значения достаточно вычислить лишь один хеш. В сервере меток времени поиск значения с нужным хешем происходил путем перебора значения итерируемого поля-добавки (nonce) в блоке данных. Как только блок, удовлетворяющий условию, найден, его содержимое нельзя изменить, не выполнив заново всей работы. И если он не является последним в цепочке, эта работа включает в себя и перевычисление всех блоков, следующих за ним.

Доказательство работы через хеширование также решает вопрос об определении версии, поддерживаемой большинством. Если голосом считается один IP-адрес, то такую схему можно скомпрометировать, если контролировать большой диапазон адресов. Схема биткоина основана на принципе "один процессор – один голос". Самая длинная из хеш-цепочек выражает мнение большинства, которое вложило в нее наибольшее количество ресурсов.

Если более половины вычислительной мощности принадлежит честным узлам, то цепочка честных транзакций будет расти быстрее и опередит любую конкурирующую цепь. Чтобы внести изменения в любой из прошлых блоков, атакующему придется выполнить заново работу над этим блоком и всеми последующими, а затем догнать и перегнать честных участников по новым блокам. Вероятность такого успеха у злоумышленника, обладающего меньшими ресурсами, экспоненциально убывает в зависимости от числа блоков.

Для компенсации возрастающей вычислительной мощи процессоров и колебания числа работающих узлов в сети сложность хеширования изменяется (примерно раз в две недели), чтобы обеспечивать равномерную скорость генерации блоков (около 10 мин.) Если они появляются слишком часто, сложность возрастает и наоборот.

Участники всегда считают истинной самую длинную версию цепочки и работают над ее удлинением. Если два узла одновременно опубликуют разные версии очередного блока, то кто-то из остальных пиров получит раньше одну версию, а кто-то другую. В таком случае каждый начнет работать над своей версией цепочки, сохранив другую на случай, если она окажется продолжена раньше. Двойственность исчезнет, как только будет получен новый блок, который продолжит любую из ветвей, и те узлы, что работали над конкурирующей версией, переключатся на нее.

Экономия дискового пространства

Как только последняя транзакция в цепочке окажется внутри достаточно старого блока, все предшествующие ей транзакции в цепочке могут быть удалены в целях очистки дискового пространства. Чтобы хеш блока остался неизменным, все транзакции в блоке хранятся в виде хеш-дерева Меркла и лишь его корень включается в хеш блока. Размер старых блоков может быть уменьшен за счет удаления ненужных ветвей этого дерева, хранить промежуточные хеши необязательно.

Заголовок пустого блока будет составлять около 80 байт. Из расчета скорости генерации блока раз в 10 мин. получаем 80*6*24*365 = 4,2 Мбайт в год. Для среднестатистического на 2008 г. компьютера с 2 Гбайт оперативной памяти, с учетом закона Мура, предсказывающего рост на 1,2 Гбайт в год, хранение данных не будет проблемой, даже если все заголовки блоков будут находиться в памяти.