Технология блокчейн для мобильных устройств и Интернета вещей

Konstantin Zhidanov, Sergey Bezzateev, Alexandra Afanasyeva, Mikhail Sayfullin,
Sergey Vanurin, Yulia Bardinova, Aleksandr Ometov
aleksandr.ometov@tuni.fi
Enecuum HK Limited, Hong Kong; ITMO university, Russia; Tampere University, Finland

Расширенная аннотация

Внедрение Bitcoin автором Satoshi Nakamoto в 2008 году оказало значительное влияние на цифровое общество [1]. В качестве первого шага Bitcoin-подобные криптовалюты казались чрезвычайно инновационной альтернативной финансовой парадигмой. Однако в основе Bitcoin лежит технологический прорыв: технология блокчейна. Приложения, которые раньше могли работать только через доверенные централизованные системы, теперь могут работать без какого-либо постоянного подключения к удостоверяющему центру, сохраняя при этот же уровень безопасности и улучшенную общую функциональность системы [2]. Эта отличительная особенность вывела блокчейн за пределы обычной области криптовалюты [3].

Основная идея самого блокчейна заключается в концепции доверия [4]. Эта идея основана на том факте, что стороны, взаимодействующие в системе, не обязательно знают или доверяют друг другу, но все же имеют возможность безопасно осуществлять операции. Использование блокчейна устраняет необходимость участия и постоянного обслуживания со стороны централизованного «доверенного» центра, что позволяет сети работать распределенным образом. В соответствии со своим названием, записи транзакций между узлами в сети блокчейна организованы в структуру данных, называемую «блоками». Последовательность блоков упорядочена в строго возрастающем порядке времени с помощью стиля данных подобного связанного списка, называемым цепочкой блоков (chain of blocks), то есть «блокчейн» («blockchain»). Блокчейн поддерживается добавлением только локальных копий самого себя узлами, участвующими в реплицированном процессе консенсуса. Из-за свойства неизменяемости блокчейна его можно абстрагировать как транзакционную систему, которая позволяет формировать консенсус среди его участников [5]. Консенсус обладает уникальными вероятностными свойствами и может использоваться в качестве фундаментального строительного блока для промежуточного программного обеспечения, которое предлагает как детерминированный, так и вероятностный консенсус.

Большая часть операций блокчейна основана на специально разработанных устройствах - майнерах, то есть узлах, пытающихся решить вычислительные головоломки, или же достичь Proof-of-Work (PoW) [6] для создания нового блока и получить прибыль в виде денежной компенсации за вычисления. Вкратце, блок содержит «одноразовые номера» («nonce»), которые майнер должен

установить таким образом, чтобы хеш всего блока был меньше известной цели, которая обычно очень мала. Сложность майнинга должна регулироваться динамически в течение всего срока службы системы [7].

В настоящее время в мире насчитывается около 2,71 миллиарда смартфонов, и среднестатистический смартфон может обрабатывать 2 миллиарда операций с плавающей запятой в секунду (FLOPS), что оставляет нам постоянно неиспользуемые 5 EFLOPS. Эта мощность может использоваться в процессах публикации и проверки транзакций, смарт-контрактах или распределенном хранилище. Практически любой современный смартфон уже может быть частью Proof of Activity (PoA) и выполнять связанные криптографические примитивы.

Стоит отметить, что использование ограниченных ресурсами устройств обычно недооценивается в отношении блокчейна. Функция майнинга не является наиболее эффективным использованием этих устройств из-за вычислительных ограничений и ограничений по мощности, но концепция, известная как Proof-of-Stake (PoS), предоставила возможность для использования таких ограниченных ресурсами устройств. В этой концепции узлы PoS не выполняют роль майнеров для решения сложных задач. При использовании PoS «держатели стейка» («stakeholders») подтверждают транзакции и блоки на основе своей «доли» в системе, и поэтому использование устройства с ограниченными ресурсами является естественным шагом вперед. Роль смартфонов заключается в том, чтобы оплачивать только операционные сборы сети без участия в реальном майнинге.

Мы предлагаем новый протокол, построенный на Bitcoin, путем объединения компонента PoW с системой типа PoS. PoA зарекомендовал себя как более защищенный от известных практических атак с относительно низким использованием ресурсов связи и хранения. В PoA майнинг обычно выполняется традиционным способом PoW. Однако добытый блок не содержит транзакций: он состоит из заголовка и адреса вознаграждения. После процесса майнинга работа системы переходит в режим PoS. Несколько держателей стейка (в нашем случае смартфоны) выбираются случайным образом для подписи (проверки) вновь созданного блока. После того, как все в группе подписывают блок, он добавляется в блокчейн. Если некоторые из «валидаторов» не участвовали в процессе валидации, блок отбрасывается, и используется следующий, основанный на PoW, и процедура повторяется. Затем вознаграждение распределяется между активными валидаторами PoS и майнерами PoW.

Подход к решению и основные полученные результаты

Основным вкладом этой работы является набор протоколов под названием «Trinity». Он позволяет использовать умную комбинацию PoA, PoS и PoW, направленную на привлечение мобильных устройств для работы блокчейна, что является основной новизной. Для решения проблемы применяются методы криптографии и натурного моделирования.

Список основной использованной литературы по теме исследования:

1. Christopher D. Manning, Prabhakar Raghavan and Hinrich Schütze, Introduction to Information Retrieval. Cambridge University Press. 2008.

2. Cliche M. “BB_twtr at SemEval-2017 Task 4: Twitter Sentiment Analysis with CNNs and LSTMs”, Proceedings of the 11th International Workshop on Semantic Evaluation (SemEval-2017), pp. 572–579, 2017.

3. Santos C., Gatti M. “Deep convolutional neural networks for sentiment analysis of short texts”, Proceedings of COLING 2014, the 25th International Conference on Computational Linguistics: Technical Papers, pp. 69–78, 2014.

4. Jurafsky D. Martin J. “Naive Bayes and Sentiment Classification,” in Speech and Language Processing, draft of August 7, 2017.

5. Mikolov T., Chen K., Corrado G., Dean J. “Efficient estimation of word representations in vector space”, arXiv preprint arXiv:1301.3781, 2013.

6. Mikolov T., Sutskever I., Chen K., Corrado G. S., Dean J. “Distributed representations of words and phrases and their compositionality”, Advances in Neural Information Processing Systems, pp. 3111-3119, 2013.

7. Mikolov T., Yih W., Zweig G. “Linguistic regularities in continuous space word representations”, Proceedings of the 2013 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, pp. 746-751, 2013.