



Contribution ID: 197

Type: Sectional reports

## Разработка децентрализованной платежной системы на основе технологии blockchain с учетом специфики мобильных платформ

*Tuesday, 11 September 2018 15:45 (15 minutes)*

Интернет находится в центре революций: централизованные проприетарные сервисы подвергаются замене на их децентрализованные аналоги со свободными лицензиями; доверенные третьи стороны юридических и финансовых договоров заменяются верифицируемыми вычислениями; неэффективные монолитные сервисы уступают место одноранговым алгоритмическим рынкам. Bitcoin, Ethereum и другие сети, фундаментом которых является технология blockchain, доказали полезность децентрализованных регистров транзакций. Имея в основе децентрализованные, открытые базы данных, они поддерживают выполнение сложных «умных» контрактов (smart contracts) и обслуживают крипто-активы стоимостью десятки миллиардов долларов. Эти системы являются первыми экземплярами межсетевых открытых сервисов, в которых участники образуют децентрализованную сеть, предоставляющую полезные услуги для коммерции, без централизованного управления или доверенных лиц. Парадигма открытости и децентрализации коснулась не только мира коммерции, но и систем хранения и обработки больших объемов данных. InterPlanetary File System показала полезность адресации контента путем децентрализации самой всемирной паутины, обслуживая миллиарды файлов, используемых в глобальной одноранговой сети. Но достижение децентрализации и ухода от доверенных третьих лиц обернулось высокими требованиями к ресурсоемкости узлов сети и потерей масштабируемости, что препятствует массовой адаптации данных систем. В особенности данная проблема проявляется в виде обхода стороной блокчейн-технологиями мобильных платформ. Между тем, в октябре 2016 использование интернета мобильными и планшетными устройствами впервые превысило ПК по всему миру в соответствии с информацией от независимой веб-аналитической компании StatCounter<sup>1</sup>. В дальнейшем тенденция роста числа мобильных узлов в сети будет сохраняться. Проблема масштабируемости не дает возможностей конкурировать с централизованными системами электронных платежей, таких как Visa, которая обеспечивает обработку порядка 65000 транзакций в секунду<sup>2</sup>. В частности, это ограничивает интеграцию с «интернетом вещей» – перспективного направления цифровой экономики.

Целью данной работы является разработка распределенной сети на основе blockchain для мобильных платформ. Выдвигается концепт для преодоления вышеуказанных ограничений текущих blockchain-проектов. Уход от таких механизмов верификации как в Ethereum и Bitcoin, использующих для достижения консенсуса между участниками сети сложные вычислительные алгоритмы. В качестве их замены выступают ресурсоэффективные алгоритмы консенсуса Proof-of-Stack. Проблемы бесконечного роста цепочки блоков находится в плоскости организации распределенного хранения данных: эффективного алгоритма выбора массива блоков для хранения узлом с учетом необходимого коэффициента репликации. Подсети на основе системы каналов «узел-узел» для микроплатежей призваны решить проблему масштабируемости.

Ключевые слова: blockchain, децентрализованные системы, криптография.

**Primary author:** ИЛЮХИН, Андрей (Dubna International University)

**Co-author:** Dr NIKONOV, Eduard (LIT JINR)

**Presenter:** ИЛЮХИН, Андрей (Dubna International University)

**Session Classification:** 4. Scientific, industry and business applications in distributed computing systems, education

**Track Classification:** 4. Scientific, industry and business applications in distributed computing systems