# РАЗРАБОТКА ДЕЦЕНТРАЛИЗОВАННОЙ ПЛАТЕЖНОЙ СИСТЕМЫ НА ОСНОВЕ ТЕХНОЛОГИИ BLOCKCHAIN С УЧЕТОМ СПЕЦИФИКИ МОБИЛЬНЫХ ПЛАТФОРМ

**А.А. Илюхин [1, a], Э.Г. Никонов [1, 2]**

[1] *Государственный Университет «Дубна», Дубна, Российская Федерация*

[2] *Объединенный институт ядерных исследований, Дубна, Российская Федерация;*

E-mail: [a] a.iluhin@nordavind.ru

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; 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 и обслуживают крипто-активы стоимостью десятки миллиардов долларов. 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 веб-аналитической компании StatCounter. В дальнейшем тенденция роста числа мобильных узлов в сети будет сохраняться. В данной статье рассматриваются подходы к разработке распределенной сети на основе blockchain для мобильных платформ. Выдвигается концепт по модификации ресурсоэффективного алгоритма консенсуса Proof-of-Stack. Проблемы бесконечного роста цепочки блоков находятся в плоскости организации распределенного хранения данных: отсутствия 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, распределенные системы, децентрализованные платежные системы.

# 1. Виды консенсусов

Потребность сторон финансового или юридического соглашения в регуляторе, добросовестность которого трудно проверить, при обеспечении надежного выполнения групп операций – транзакций – создает определённые проблемы. Основой данной схемы является доверие – механизм, который, строго говоря, не дает никаких гарантий точного исполнения, даже в случае, если в качестве регулятора выступает государственный институт. Исключение центрального элемента и переход на децентрализованную систему регулирования соглашений избавляет от данной проблемы. При таком подходе задача безопасности, в частности аутентификация, успешно решается криптографическими алгоритмами. Но нетривиального подхода требует разработка инструмента, который обеспечит договоренность между участниками системы относительно ее текущего состояния и правил его изменения, то есть достижения консенсуса между участниками.

Данная проблема совместно с развитием цифровых технологий и криптографических алгоритмов предрекли появление blockchain: технологии надежного распределенного хранения достоверных записей. Blockchain является базой данных, которая формируется как постоянно растущая линейная структура, состоящая из блоков с записями о всех транзакциях. Информация в блоках носит открытый характер, но защищена от изменений при помощи хеш-дерева (дерево Меркла) и цифровых подписей. База синхронизируется по формальным правилам консенсуса и реплицируется между всеми участниками распределенной системы [1]. Применительно к blockchain достижение консенсуса заключается в решении классической задачи византийских генералов [2]. Учитывая, что майнеры географически распределены и времена создания блоков от различных майнеров сильно разнятся, возможно появление множества альтернативных цепочек блоков. Следовательно, blockchain из линейной структуры реорганизуется в древовидную. Цель консенсуса – обеспечить согласованное принятие каждым узлом сети одной определенной цепочки, соответствующей правилам консенсуса.

На текущий момент разработаны следующие алгоритмы консенсуса:

- Proof-of-Work (Pow) – «доказательство выполненной работы». Первый вид консенсуса, используемый в первой криптовалюте – Bitcoin. Достижение консенсуса представляет собой подбор для нового блока хеш-значения, удовлетворяющего определенному виду. Таким образом, каждый блок показывает, что была проделана определенная работа (затрачены определенные вычислительные ресурсы) по его нахождению.

- Семейство «Доказательство доли владения»: Proof-of-Stake (PoS), Delegated Proof-of-Stake (DpoS), Leased Proof-of-Stake (LpoS). Метод защиты криптовалюты, при котором вероятность генерации блока прямопропорциональна наличию определенной суммы. Помимо того, что криптовалюты Proof-of-Stake являются более энергоэффективными, чем Proof-of-Work, стимулы генераторов блоков также различаются. Proof-of-Work майнер может потенциально не владеть ни одной из валют, которую майнит. Это означает, что его интересы могут расходиться с держателями монет. Майнера заботит краткосрочная окупаемость оборудования и быстрая продажа монет. Тем не менее, Proof-of-Stake не является идеальным вариантом для распределенного консенсус-протокола. Существует проблема «ничего на кону» (nothing-on-stake), при которой одна и та же ставка применяется к нескольким конкурирующим цепочкам, что мешает достижению консенсуса [3].

- Гибридные: Proof-of-Burn (PoB) – «доказательство сжигания», Proof-of-Activity (PoA) – «доказательство активности». «Доказательство сжигания» декларирует, что для приобретения права на генерацию блоков криптовалюты необходимо уничтожить некоторое ее количество, полученной в системе с доказательством выполнения работы. Под «сжиганием» подразумевается отправка майнером некоторого количества средств на специальный адрес, с которого невозможно их вернуть или потратить. Proof-of-Activity предполагает совместное участие майнеров Proof-of-Work и Proof-of-Stake с разделением ролей. Первые обеспечивают генерацию новых монет за счет сложности такого типа майнинга. Вторые формируют и подтверждают массив транзакций, который будет включен в блок.

- Proof-of-Capacity (PoC), Proof-of-Spacetime/Proof-of-Replication. Концепт PoC создает необходимость майнеру выделять значительный объем дискового пространства для генерации нового блока. При помощи схемы доказательства с нулевым разглашением, усовершенствованная версия PoC – PoS – с некоторой вероятностью гарантирует для определенного периода времени наличие у майнера массивов данных для генерации [4].
- Proof-of-Authority (PoAuthority) – «доказательство полномочий». Записи в распределенный реестр могут добавлять исключительно узлы, которые получили на это изначально разрешение

## 2. Подходы к масштабируемости

Проблема согласованности узлов относительно состояния blockchain не является главным камнем преткновения на пути замены фиатных валют криптовалютами. Сатоши Накамото, создатель протокола Bitcoin, в 2009 году утверждал, что проблема масштабируемости решится сама собой при помощи закона Мура. Но его надежды не оправдались и на текущий момент данный вопрос стал наиболее острым для криптовалютной отрасли [5]. Суть проблемы в том, что каждый полнофункциональный узел в сети должен обрабатывать каждую транзакцию. Blockchain в силу своего устройства является децентрализованной технологией. Это значит, что не существует некого центрального органа, отвечающего за сохранение системы и её защиту. Вместо этого каждый отдельно взятый узел в сети отвечает за обеспечение защиты системы, обрабатывая каждую транзакцию и сохраняя копию всего состояния системы. В результате получается низкий темп обработки транзакций в сравнении с современными централизованными платежными системами.

**Каналы микроплатежей**

Идея состоит в том, чтобы вынести обработку регулярных транзакций за пределы blockchain. Канал микроплатежей – это прямой обмен транзакциями, организованный между двумя узлами основной сети, в которых данные узлы фигурируют как отправитель и принимающая сторона. Время работы канала устанавливается отправителем произвольно, при этом получатель может досрочно закрыть канал. При этом сумма, участвующая в обмене фиксирована на все время существования канала.

Алгоритм открытия канала:

Принимающая сторона генерирует новую пару ключей для электронной подписи и передает открытый ключ клиенту. Отправитель в свою очередь генерирует новую пару ключей и использует свой открытый ключ и открытый ключ принимающей стороны для формирования multisignature адреса 2-из-2. Отправитель формирует транзакцию номер один, в которой он отправляет сумму обмена на multisignature адрес. Подписывает ее, но не распространяет в сеть blockchain, поскольку принимающая сторона может быть недобросовестной и отказаться подписывать любые транзакции для дальнейшей передачи. В связи с этим отправитель формирует транзакцию номер два, где монеты с multisignature адреса отправляются на адрес, который он контролирует сам. Время блокировки устанавливается в ней таким образом, чтобы транзакция могла быть подтверждена через сутки. Эта транзакцию отправителем не подписывается, а отправляет принимающей стороне. Принимающая сторона удостоверяется, что клиент может забрать всю сумму обмена не раньше, чем через сутки, и подписывает транзакцию своим ключом. Подпись передается отправителю. Теперь отправитель имеет возможность доподписать транзакцию своим ключом и гарантированно забрать монету обратно, если принимающая сторона решит отказать в дальнейшем взаимодействии. Отправитель распространяет транзакцию номер один в blockchain.

Для отправки первого платежа отправитель формирует транзакцию номер три, в которой сумма обмена с multisignature адреса распределяется между двумя выходами: первый – это платеж на адрес принимающей стороны, второй — это сдача на собственный адрес. Отправитель подписывает транзакцию номер три своим ключом и передает принимающей стороне. Для отправки всех последующих платежей отравитель изменяет выходные значения транзакции номер три, соответственно, переподписывает ее и передает принимающей стороне

уже только саму подпись и сумму изменения. Данный подход решает проблему пропускной способности, поскольку в таком случае блокчейн может масштабироваться под больший объём транзакций.

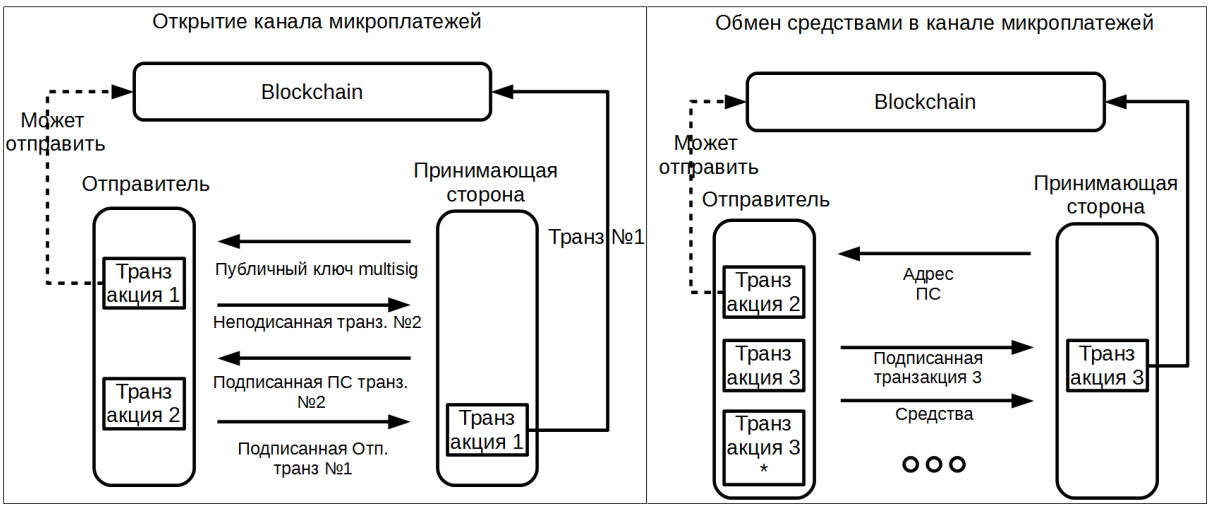


Рисунок 1. Канал микротранзакций

Более того, поскольку транзакция происходит, как только её обработал платёжный канал, а не тогда, когда блок получает подтверждение, каналы микроплатежей решают и проблему скорости, позволяя избавиться от типичных задержек [6].

**Sharding**

В основе sharding лежит схема, в соответствии с которой общее состояние блокчейна разделяется на сегменты. Каждая часть состояния хранится и обрабатывается разными узлами в сети. Каждый узел обрабатывает лишь малую часть состояния, делая это параллельно с остальными. Sharding блокчейна аналогичен фрагментации традиционной базы данных, за исключением крайне сложной проблемы, состоящей в необходимости сохранять безопасность и аутентичность в рамках децентрализованного набора узлов. Данный подход имеет множество нерешенных вопросов и находится на стадии теоретической проработки.

**Направленные ациклические графы**

Направленный ациклический граф (НАГ) представляет собой структуру данных, гарантирующую невозможность начать движение в любой вершине и следовать череде рёбер, которая в итоге возвращается к этой вершине (то есть невозможны замкнутые циклы). Это позволяет иметь последовательность узлов (или вершин) в топологическом порядке. Предпосылка разработки протоколов на основе направленных ациклических графов, таких как IOTA's Tangle, состоит в том, чтобы полностью избавиться от глобальной линейной структуры блокчейна в пользу структур данных НАГ, что позволит лучше поддерживать состояние системы.

Tangle – это алгоритм консенсуса НАГ, который использует IOTA. Чтобы отправить транзакцию, необходимо подтвердить две любые дошедшие до узла предыдущие транзакции. Консенсус по принципу «два к одному» укрепляет справедливость транзакций. Поскольку консенсус определяется транзакциями, теоретически, если кто-то может генерировать треть всех транзакций, они могут захватить сеть. В IOTA введена «двойная проверка» всех транзакций сети на централизованном узле «координатор» [7].

## 3. Предлагаемые методы решения

**Разработка консенсуса.**

Учитывая высокие темпы развития вычислительной мощности процессоров, объема оперативной памяти относительно объемов запоминающих устройств, последние могут оказаться самым слабым звеном в работе blockchain, принимая во внимание его неограниченный рост. Очевидна необходимость в минимальном объеме blockchain на конкретном узле при условии сохранения его полной функциональности. Фактически весь blockchain необходим участнику сети только на этапе начальной синхронизации, то есть при первом подключении к сети. На этой стадии необходимо получить текущее состояние blockchain, убедившись что оно было достигнуто согласно правилам консенсуса. После инициализирующей стадии для проверки новых транзакций достаточно хранить только те транзакции, у которых имеются не потраченные выходы. Но ограничиться лишь не потраченными выходами нельзя – узел должен способствовать синхронизации новых участников. Предлагается доработать консенсус Proof-of-Stake, включив в процесс генерации блока помимо хеша предыдущего блока зависимость от некоторого набора данных из других блоков, отбор которых определяется некоторой функцией. На каждой итерации набор блоков должен изменяться и быть не прогнозируемым, чтобы помешать процедуре упреждающего майнинга. Таким образом обеспечивается стимул майнера хранить как можно больше истории, повышая свои шансы встретить необходимый набор блоков. Ниже представлена схема.

Данная схема не идеальна, так как каждый майнер будет выбирать случайным образом часть, которую будет хранить. Имеется вероятность, что некоторая часть blockchain не будет присутствовать ни на одном узле. Более того, нужно обеспечить нужный коэффициент репликации каждого блока. Для решения этой задачи необходима адаптация Proof-of-Replication.

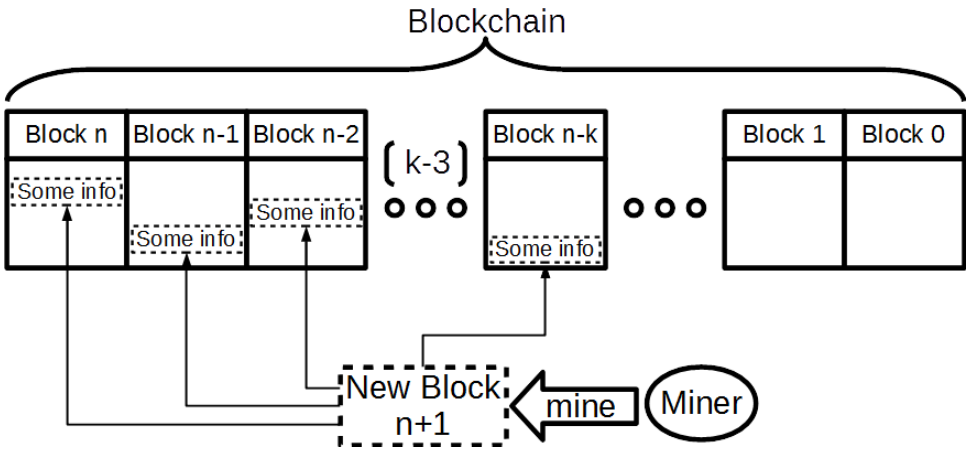


Рисунок 2. Зависимость генерации нового блока от информации в предшествующих блоках

**Разработка механизмов масштабируемости**

Для решения задачи масштабирования необходимо устройство blockchain, наделённое защитой, аналогичной той, что присутствует у bitcoin и ethereum, и при этом позволяющее системе функционировать так, чтобы каждому отдельно взятому узлу не требовалось обрабатывать больше определённого процента от всего объёма транзакций в сети. Иными словами, нам нужен механизм, позволяющий ограничить число узлов, необходимых для подтверждения достоверности и аутентичности каждой транзакции, не вызывающий утрату доверия. Так как каналы микроплатежей значительно снижают общий объем blockchain по отношению к sharding и механизмам на основе направленных ациклических графов, их использование представляется наиболее перспективным. Ограничение двухузловой коммуникации предлагается обходить при помощи организации трансляторов – узлов сети, которые выступят связующим звеном между подключенными к нему пользователями.

Для защиты данного вне-blockchain слоя от атак предлагается использовать алгоритм Eigentrust++.

## Список литературы

[1] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. Available at: https://bitcoin.org/bitcoin.pdf. (accessed 10.06.2016)

[2] Swan M. Blockchain: Blueprint for a New Economy // O'Reilly Media, Inc. – 2015. – pp. 1-7.

[3] Sunny King, Scott Nadal. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake/ Available at: https://peercoin.net/assets/paper/peercoin-paper.pdf. (accessed 27.07.2016)

[4] Stefan Dziembowski, Sebastian Faust, Vladimir Kolmogorov, Krzysztof Pietrzak. Proofs of Space. Available at: https://eprint.iacr.org/2013/796.pdf. (accessed 11.04.2017)

[5] Satoshi Nakamoto. Development & Technical Discussion. Available at: https://bitcointalk.org /index.php?topic=12.msg45#msg45. (accessed 4.08.2016)

[6] Joseph Poon, Thaddeus Dryja. The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. Available at: https://lightning.network/lightning-network-paper.pdf. (accessed 2.09.2016)

[7] Popov S. The Tangle. Available at: https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0 EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf (accessed 19.05.2018)

# DEVELOPMENT OF BLOCKCHAIN BASED DECENTRALIZED PAYMENT SYSTEM ACCORDING TO MOBILE PLATFORM SPECIFICS

**A.A. Ilukhin [1, a], E.G. Nikonov [1, 2]**

[1] *Dubna State University, Dubna, Russian Federation*

[2] *Joint Institute for Nuclear Research, Dubna, Russian Federation*

E-mail: [a] a.iluhin@nordavind.ru

The internet is in the middle of a revolution: centralized proprietary services are being replaced with decentralized open-license counterparts; trusted parties of legal and financial agreements replaced with verifiable computation. Bitcoin, Ethereum and other blockchain networks have proven the utility of decentralized transaction ledgers. Based on decentralized open databases, these public ledgers process sophisticated smart contract applications and transact crypto-assets worth tens of billions of dollars. However, the achievement of decentralization and getting rid of trusted third parties has resulted in high demands on the resource intensity of network nodes and scalability loss, which prevents the mass adaptation of these systems. In particular, this problem manifests itself as blockchain-technology bypassing of mobile platforms. Meanwhile, in October 2016, the Internet usage with mobile and tablet devices surpassed PCs one around the world in accordance with information of StatCounter web analytics firm. The trend of mobile nodes growth in the network will continue in the future. Approaches to developing blockchain-based distributed networks for mobile platforms is suggested in this article. The concept of modification of resource-efficient consensus algorithm Proof-of-Stack is proposed. Blockchain infinite growth problems lies in distributed data storage organization: the lack of an efficient algorithm for selecting an array of blocks for storage by a node, while taking into account the required replication factor. Micro-payment node-to-node channel subnets are adapted to solve the scalability problem.

Keywords: blockchain, distributed systems, decentralized payment systems.