

ТЕНДЕНЦИИ РАЗВИТИЯ БЛОКЧЕЙН СИСТЕМ

Гумеров Эмиль Абильхаирович,

канд. техн. наук, доцент,

старший преподаватель кафедры информационных систем и технологий,

e-mail: gumerovemil@yandex.ru,

Московский финансово-юридический университет (МФЮА), г. Москва

В статье проведён анализ развития блокчейн систем, отмечено, что блокчейн системы развиваются в направлении совершенствования пользовательских интерфейсов и повышения скорости работы. Отмечаются достижения в разработке более совершенных алгоритмов консенсуса, в создании собственных, приспособленных к блокчейн системам, сетевых протоколов. Обосновывается тезис о том, что гибкость технологии блокчейн способствует стремительному расширению областей применения блокчейн систем. Показывается тенденция расширения применения современными банками криптосистем распределённого реестра: наряду с системами Ripple и Stellar, специально разработанными для банковской деятельности, применяются стейблкоины - криптовалюта, привязанные к активам. Рассматривается роль профессиональных программных продуктов корпорации IBM в расширении области применения систем распределённого реестра в управлении предприятиями и организациями. Проведён сравнительный анализ криптосистем распределённого реестра Ripple и Stellar с существующей системой межбанковских каналов SWIFT. Показано существенное преимущество криптосистем распределённого реестра в скорости выполнения транзакций и в удобстве пользовательских интерфейсов.

Ключевые слова: блокчейн система, блокчейн технология, криптосистема, распределённый реестр, алгоритм консенсуса, ациклический граф, стейблкоин, сетевой протокол

DEVELOPMENT TRENDS OF BLOCKCHAIN SYSTEMS

Gumerov E.A.,

cand. tech. sci., Associate Professor, lecturer, department

of information systems and technologies,

e-mail: gumerovemil@yandex.ru,

Moscow University of Finance and Law (MFUA)

The article analyzes the development of blockchain systems, it is noted that blockchain systems are developing in the direction of increasing user convenience, including in terms of user interfaces and increasing speed of work. There are achievements in the development of more sophisticated consensus algorithms, in the creation of proprietary networked protocols adapted to blockchain systems. It justifies the thesis that the flexibility of the blockchain technology contributes to the rapid expansion of the areas of application of the blockchain systems. For example, there is a tendency to expand the use of distributed registry cryptosystems by modern banks. Along with the Ripple and Stellar systems, specially designed for banking, there are steakloikoiny, cryptocurrency, tied to assets. IBM professional software products play a significant role in expanding the use of distributed registry cryptosystems in the management of enterprises and organizations in all spheres of life. A comparative analysis of the cryptosystem of the Ripple and Stellar distributed registry with the existing system of interbank SWIFT channels has been carried out. The essential advantage of cryptosystems of the distributed registry in speed of execution of transactions and in convenience of user interfaces is shown.

Keywords: blockchain system, blockchain technology, cryptosystem, distributed registry, consensus algorithm, banking, acyclic graph, stablecoin, consensus algorithm, network protocol, acyclic graph

DOI 10.21777/2500-2112-2019-2-59-63

Сопределенными допущениями можно выделить четыре поколения блокчейн систем. Это разделение является условным и не претендует на результирующую классификацию, но позволяет выделить характерные особенности развития блокчейн систем.

Первым поколением блокчейн систем является классический блокчейн криптовалюты биткоина. Он характеризуется алгоритмом консенсуса по проделанной работе (протокола Proof-of-Work, «доказательство выполненной работы»). Открытый ключ электронной подписи хранится в предыдущем блоке и защищён хэш функцией (закрытый ключ находится в новом блоке). Ключевой особенностью блокчейн систем первого поколения является выполнение транзакции в сети блокчейн по протоколу Proof-of-Work.

Вторым поколением блокчейн систем является блокчейн криптовалюты Ethereum. Разработчик, Виталик Бутерин, предложил гениальную идею смартконтрактов, имеющих алгоритмы автоматической проверки выполнения договорных обязательств и логических условий. Это позволило применить блокчейн системы в новых областях деятельности, в создании принципиально новых прикладных программ.

Применён протокол Casper, ключевая особенность которого – изменение алгоритма консенсуса: переход с используемого в биткоине протокола Proof-of-Work (PoW, «доказательство выполненной работы») на Proof-of-Stake (PoS, «доказательство владения»). Скорость транзакций увеличена до 30 в секунду.

Программное обеспечение платформы Ethereum располагает всеми инструментами для создания пользователем своей прикладной программы, в том числе программы на основе блокчейн Ethereum.

Особенностью блокчейн систем *третьего поколения* криптосистем распределённого реестра, как считают отдельные авторы [1], является применение ациклического графа вместо блокчейна или совместно с блокчейном. В криптосистемах ациклического графа транзакции осуществляются мгновенно, поскольку их не нужно собирать в блоки. Структура называется DAG (directed acyclic graph) – это структура блоков с топологическим деревом в основе. Блоки могут подтверждать не одну, а несколько транзакций, что помогает избежать так называемой «двойной траты». Ациклические графы применяются, например, в криптосистеме для промышленного интернета ЮТА, занимающая в данное время 16-ое место по рыночной капитализации (896 млн \$). Достигнута скорость 1000 транзакций в секунду.

В криптосистемах третьего поколения применён алгоритм консенсуса DPoS (Delegated Proof of Stake). По этому алгоритму блоки, подтверждающие консенсус определяются голосованием с разделением голосующих и валидирующих участников: участники используют свои токены, чтобы выбирать валидаторов, которые за вознаграждение проверяют и добавляют блоки. Криптосистема обеспечивает безопасность и высокую скорость транзакций, а распределённый реестр, являясь распределённой базой данных, обеспечивает прозрачность, выполнение транзакций независимо от национальных границ и усиливает свойство безопасности благодаря фиксации параметров транзакций на множестве компьютеров.

В настоящее время существенно увеличился поток работ, посвящённый практическому применению криптосистем распределённого реестра [4, 9, 10] и вопросам стандартизации криптосистем распределённого реестра, например [5, 6]. В работе [3] показана значимость криптосистем распределённого реестра для развития всех сторон жизни, в работе [8] блокчейн системы рассматриваются как новая парадигма институциональной экономики.

Рассмотрим новые технологии работы блокчейн систем на примере платформы *Seele* [12], которую разработчики данной платформы относят к четвертому поколению. Платформа поддерживает управление различными сценариями для бизнеса и интернета вещей. К новым решениям платформы *Seele* можно отнести следующие:

1. Применен новый, специально разработанный алгоритм *нейронного консенсуса*, который существенно повышает безопасность системы. Алгоритм работает по принципу зрительного анализатора человека: сначала схватывается вся картина, а потом она детализируется.

2. Применен специально разработанный для платформы *Seele* скоростной транспортный протокол интернета QVIC и протокол VHTTP для сети «передачи ценностей».

3. Платформа содержит множество блокчейн систем, которые можно специализировать для решения различных задач, в том числе:

- контроль выполнения финансовых операций;
- управление предприятием;

- хранение прав собственности, авторских прав, прав на мультимедиа контент;
- управление беспроводной связью, в том числе спутниковой;
- управление страховой компанией;
- управление туристической компанией.

На платформе *Seele* возможна информационная связь между цепочками блоков различных блокчейнов. Имеется общее электронное хранилище исходных данных для программ-оракулов и смартконтрактов. Заявленная скорость работы платформы составляет 1 млн транзакций в секунду. Однако на сегодняшний день предварительные испытания проекта *Seele* не завершены, что затрудняет проверку эффективности декларированных возможностей блокчейн системы.

Возникла и укрепляется тенденция использования традиционными банками криптосистем распределённого реестра, в частности, блокчейн технологий. Это показательно, так как именно банки выражали в большей степени отрицательное отношение относительно криптовалюты на начальном этапе ее появления. Примеры использования банками криптосистем распределённого реестра:

- межбанковские расчёты;
- финансовый холдинг «UBS Group AG» в Швейцарии использует «монету для коммунальных расчетов», то есть криптосистему, которая конвертирует криптовалюту в депозиты наличных денег в центральных банках;
- финансовый холдинг «Credit Suisse Group AG» использовал блокчейн в банке для повышения эффективности операции;
- «Bank of America» использовал технологию распределённого реестра для безопасного хранения депозитов [11].

Ряд классических банков Европы проявил понимание рынка криптовалют и пошел навстречу своим клиентам и стал оказывать поддержку им в сделках с криптовалютами. Речь идет о таких банках, как швейцарские Falcon Bank и Vontobel, Fidor Bank в Германии, а также Bank Frick со штаб-квартирой в Лихтенштейне.

Революционным для применения криптосистем распределённого реестра является создание крупным финансовым холдингом *JP Morgan Chase* собственной криптовалюты для мгновенного проведения крупных транзакций [7]. Блокчейн для криптоплатформы разработан корпорацией IBM.

Токен *JPM Coin* мгновенно выполняет операции между клиентами *JP Morgan Chase*, обслуживая 80 % компаний из списка Fortune 500. При использовании банковских переводов в сети SWIFT, требуется несколько дней на одну транзакцию. Новая валюта JP Morgan может существенно повлиять и даже преобразить традиционную финансовую систему. Однако, банковский JPM Coin не будет доступен розничным инвесторам. Токен смогут использовать только институциональные клиенты JP Morgan, такие как корпорации, банки и брокеры-дилеры, причём используется только одно преимущество блокчейн технологий: мгновенное выполнение транзакций, отказываясь от прозрачности, открытости, от привлечения розничных инвесторов.

Банк использует концепцию популярных на сегодняшний день *стейблкоинов*, рынок которых в данное время показывает взрывной рост. Монета JPM Coin подлежит обмену на один доллар США. Клиент получает JPM Coin после внесения на счет долларов. После снятия долларов со счета токены уничтожаются. Другим преимуществом банковского токена станут операции с ценными бумагами. Например, банк JP Morgan уже использовал блокчейн для создания виртуальной симуляции депозитного сертификата на 150 миллионов долларов для канадского банка.

Критики подчеркивают, что компаниям, выпускающим стейблкоины, необходимо где-то держать соответствующий объем фиатной валюты (например, бумажных денег), и эти средства в определенных случаях может конфисковать правительство, но банк JP Morgan предусмотрительно берёт хранение фиатной валюты на себя.

Лидером по разработке блокчейн систем для банковской деятельности является корпорация IBM. Её платформа *Blockchain World Wire* вызвала интерес среди банков, шесть из которых уже подписали договор об ее использовании для выпуска собственных стейблкоинов. Среди них бразильский Banco Bradesco, южнокорейский Bank Busan, и филиппинский Rizal Commercial Banking Corporation, японский банк Mizuho Financial Group. Платформа *Blockchain World Wire*, обеспечивает международные банков-

ские расчеты в режиме реального времени, используя токен XLM проекта децентрализованной банковской криптосистемы распределённого реестра *Stellar*, чтобы конкурировать с системой международных платежей аналогичной, но централизованной криптовалютой *Ripple* [2]. По мнению разработчиков, *World Wire* легко интегрируется с любой существующей платёжной системой и поддерживает платежи любого размера, в любое место назначения, в любом типе активов, в среде с высокой степенью защиты.

Расширяют своё применение и увеличивают свою рыночную капитализацию криптосистемы, специально разработанные как платёжные системы.

Ripple – мировая система взаимного расчёта. Криптовалюта *Ripple* представляет собой систему для межвалютных расчетов в режиме реального времени. Основными клиентами *Ripple* являются банки, использующие решение на базе программного обеспечения *xCurrent* для осуществления трансграничных платежей с возможностью отслеживания переводов в реальном времени. Заметим, что *xCurrent* – это блокчейн платформа *Ripple*, созданная для того, чтобы банки могли перемещать средства через границы быстро и эффективно с использованием *RippleNet*, блокчейна *Ripple*. Команда проекта создала новую платёжную систему, с помощью которой можно совершать платежи во всех валютах. Преимущество этой валюты в том, что ее используют банки, при этом она остаётся централизованной. На банковском рынке *Ripple* потеснила своего основного конкурента – Общество всемирных межбанковских финансовых каналов связи (SWIFT) с головным офисом в Брюсселе. Система SWIFT – фактически система управления перемещением денежных потоков в мире. Она объединяет около 11000 финансовых компаний. Рынок межбанковских платежей составляет несколько триллионов долларов США и именно на нём соперничают SWIFT и *Ripple*.

Stellar – полный клон криптовалюты *Ripple*, но без её врождённых недостатков в виде централизованного и авторитарного управления. *Stellar* является блокчейном поколения 4.0, а инфраструктура проекта легко подходит не только для выпуска собственных токенов, но и для функционирования в качестве децентрализованной крипто биржа: пользователи могут легко обмениваться криптовалютами внутри системы или конвертировать их в привычные фиатные деньги. При этом ни отправитель, ни получатель напрямую не соприкасаются с криптовалютой. Росту этой криптовалюты в значительной мере способствовало партнерство *Stellar* с компанией IBM, в рамках которого были реализованы трансграничные платежи с использованием *Stellar*.

Заключение

В статье проведен анализ тенденций развития технических решений, используемых в основе блокчейн технологий. В частности, показано, что блокчейн системы развиваются в направлении совершенствования пользовательских интерфейсов и повышения скорости работы. Проанализированы достижения в разработке алгоритмов консенсуса, а также в создании уникальных сетевых протоколов. Продемонстрированы возможности, которые открывает использование программных разработок фирмы IBM для практического использования систем распределённого реестра в управлении организацией.

Список литературы

1. Блокчейн третьего поколения (blockchain 3.0) и DAG-сети [Электронный ресурс]. Режим доступа: <https://ecrypto.ru/blokchejn/blokchejn-tretego-pokoleniya-blockchain-3-0-i-dag-seti.html> (дата обращения: 09.06.2019).
2. Бондарчук Н. Сразу шесть банков планируют запустить стейблкоины на платформе IBM Blockchain World Wire [Электронный ресурс]. Режим доступа: <https://bits.media/srazu-shest-bankov-planiruyut-zapustit-steyblkoiny-na-platforme-ibm-i-stellar/> (дата обращения: 20.04.2019).
3. Генкин А., Михеев А. Блокчейн. Как это работает и что ждет нас завтра // Пабlishер Альпина, 2018.
4. Дэниелс Джефф, Сарголзей Саман, Сарголзей Аран, Ахрам Тарек, Лапланте Филипп Интернет вещей, искусственный интеллект, блокчейн и профессионализм // Открытые системы. СУБД [Электронный ресурс]. – 2019. – № 1. – С. 14–16. Режим доступа: <https://www.osp.ru/os/2019/01/13054750/> (дата обращения: 20.04.2019).

5. *Елистратов А., Маршалко Г., Светушкин В.* Подводные камни сертификации блокчейн-решений. // Открытые системы. СУБД [Электронный ресурс]. – 2019. – № 1. – С. 21–23. Режим доступа: <https://www.osp.ru/os/2019/01/13054747/> (дата обращения: 20.04.2019).
6. *Клаудио Лима* Разработка открытых интероперабельных стандартов распределённого реестра // Открытые системы. СУБД [Электронный ресурс]. – 2019. – № 1. – С. 17–20. Режим доступа: <https://www.osp.ru/os/2019/01/13054749/> (дата обращения: 20.04.2019).
7. Крупнейший банк США JP Morgan запускает свою криптовалюту JPM Coin [Электронный ресурс]. Режим доступа: <https://mining-cryptocurrency.ru/jp-morgan-zapuskayet-kriptovalyutu-jpm-coin/> (дата обращения: 20.04.2019).
8. *Тапскотт Д., Тапскотт А.* Блокчейн-революция. Как технология, стоящая за биткойном, меняет деньги, бизнес и мир (Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World). – М.: ЭКСМО, 2017.
9. *Чеканов М., Волков Д.* Практический блокчейн // Открытые системы. СУБД [Электронный ресурс]. – 2019. – № 1. – С. 26–29. Режим доступа: <https://www.osp.ru/os/2019/01/13054746/> (дата обращения: 20.04.2019).
10. *Юсуфов Р., Чаленко Е.* Блокчейн в примерах // Открытые системы. СУБД [Электронный ресурс]. – 2019. – № 1. – С. 24–25. Режим доступа: <https://www.osp.ru/os/2019/01/13054745/> (дата обращения: 20.04.2019).
11. «Bank of America» разработал уникальную систему по хранению криптодепозитов [Электронный ресурс]. Режим доступа: <https://bitexpert.io/news/bank-of-america-razrabotal-unikalnuyu-kriptosistemu/> (дата обращения: 20.04.2019).
12. Seele. Russian Whitepaper [Электронный ресурс]. Режим доступа: «<http://icodaily.ru/whitepaper/seele-pro/>» (дата обращения: 20.04.2019).

References

1. Blockchain third generation (blockchain 3.0) and DAG-network. – URL: <https://ecrypto.ru/blokchejn/blokchejn-tretego-pokoleniya-blockchain-3-0-i-dag-seti.html> (data obrashcheniya: 09.06.2019).
2. *Bondarchuk N.* Immediately, six banks are planning to launch stablecoins on the IBM Blockchain World Wire platform. – URL: <https://bits.media/srazu-shest-bankov-planiruyut-zapustit-steyblkoiny-na-platforme-ibm-i-stellar/> (data obrashcheniya: 04.04.2019).
3. *Genkin A., Mikheev A.* Blockchain. How it works and what awaits us tomorrow // Publisher Alpina, 2018.
4. *Daniels Jeff, Sargolzey Saman, Sargolzei Aran, Ahram Tarek, Laplante Philip.* The Internet of Things, artificial intelligence, blockchain and professionalism // Open Systems. DBMS. – 2019. – № 1. – P. 14–16. – URL: <https://www.osp.ru/os/2019/01/13054750/> (data obrashcheniya: 04.20.2019).
5. *Elistratov A., Marshal G., Svetushkin V.* Pitfalls of blockchain solutions certification. // Open systems. DBMS. – 2019. – № 1. – P. 21–23. – URL: <https://www.osp.ru/os/2019/01/13054747/> (data obrashcheniya: 04.20.2019).
6. *Claudio, Lima.* Development of open interoperable distributed registry standards // Open systems. DBMS. – 2019. – № 1. – P. 17–20. – URL: <https://www.osp.ru/os/2019/01/13054749/> (data obrashcheniya: 04.20.2019).
7. The largest US bank JP Morgan launches its cryptocurrency JPM Coin. – URL: <https://mining-cryptocurrency.ru/jp-morgan-zapuskayet-kriptovalyutu-jpm-coin/> (data obrashcheniya: 04.20.2019).
8. *Tapskott D., Tapskott A.* Blokchejn-revolyuciya. Kak tekhnologiya, stoyashchaya za bitkojnom, menyaet den'gi, biznes i mir (Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World). – М.: EKSMO, 2017.
9. *Chekanov M., Volkov D.* Practical blockchain // Open systems. DBMS. – 2019. – № 1. – P. 26–29. – URL: <https://www.osp.ru/os/2019/01/13054746/> (data obrashcheniya: 04.20.2019).
10. *Yusufov R., Chalenko E.* Blockchain in examples // Open systems. DBMS. – 2019. – № 1. – P. 24–25. – URL: <https://www.osp.ru/os/2019/01/13054745/> (data obrashcheniya: 04.20.2019).
11. Bank of America has developed a unique cryptodeposit deposit system. – URL: <https://bitexpert.io/news/bank-of-america-razrabotal-unikalnuyu-kriptosistemu/> (data obrashcheniya: 04.20.2019).
12. Seele. Russian Whitepaper. – URL: “<http://icodaily.ru/whitepaper/seele-pro/>” (data obrashcheniya: 04.20.2019).