Технологии распределенных реестров и перспективы их использования в системе образования

Д. А. Качан, заместитель директора по научной работе
E-mail: kachan@giac.by
Учреждение «Главный информационно-аналитический центр Министерства образования Республики Беларусь», ул. Захарова, д. 59, 220088, г. Минск, Республика Беларусь

Аннотация. В статье рассмотрены особенности технологии распределенных реестров на базе использования децентрализованных пиринговых сетей. Подробно рассмотрена история возникновения и развития технологии распределенных реестров, проанализированы предпосылки роста ее популярности в различных сферах. Выявлены основные достоинства и недостатки технологии распределенных реестров в целом, а также децентрализованных (permissionless) и эксклюзивных (permissioned) Блокчейн-платформ в частности. Описаны принципы функционирования криптовалют на основе Блокчейн-технологии, в том числе их эмиссии (чеканки). Выявлены основные тенденции развития Блокчейн-технологии на современном этапе. Представлен анализ возможностей использования технологии распределенных реестров органами государственного управления, в том числе в системе образования, в целях повышения безопасности и автоматизации выполняемых функций.
Ключевые слова: технология распределенных реестров; Блокчейн; криптовалюта; майнинг; пиринговые сети; электронные платежи; Proof-of-Work (POW); биткоин; Proof-of-Stake (POS); смарт-контракты; информационные технологии в образовании
Для цитирования: Качан, Д. А. Технологии распределенных реестров и перспективы их использования в системе образования / Д. А. Качан // Цифровая трансформация. – 2018. – № 4 (5). – С. 44–55.

Distributed Ledger Technologies and Prospects of Their Use in the Education System

D. A. Kachan, Deputy Director of Research
E-mail: kachan@giac.by
Establishment “The Main Information and Analytical Center of the Ministry of Education of the Republic of Belarus”, 59 Zakharova Str., 220088 Minsk, Republic of Belarus

Abstract. The article discusses the features of distributed ledger technology based on the use of decentralized peer-to-peer networks. The history of the emergence and development of distributed ledger technology considered in detail, the prerequisites for the growth of its popularity in various fields are analyzed. The main advantages and disadvantages of distributed ledger technology in general, as well as decentralized (permissionless) and exclusive (permitted) blockchain platforms in particular, are revealed. The principles of functioning of cryptocurrencies on the basis of blockchain technology, including their issue (coinage) are described. The state of blockchain technologies from the point of view of technology maturity is considered. The main trends in the development of blockchain technology at the present stage are revealed. An analysis of the possibilities of using distributed ledger technology of public administration, including in the education system, in order to improve the safety and automation of functions is presented.
Key words: distributed ledger technology; blockchain; cryptocurrency; mining; peer-to-peer networks; electronic payments; Proof-of-Work (POW); bitcoin; Proof - of-Stake (POS); smart contracts; information technologies in education
For citation: Kachan D. A. Distributed Ledger Technologies and Prospects of Their Use in the Education System. *Cifrovaja transformacija* [Digital transformation], 2018, 4 (5), pp. 44–55 (in Russian).

1. Введение. Технология распределенных реестров (далее — Блокчейн) вызывает огромный интерес как у представителей бизнес-сообщества, так и органов государственно-

го управления. На данную технологию возлагают большие надежды, считая ее прорывной в части обеспечения надежности хранения данных, обеспечения информационной безопасности. На Всемирном экономическом форуме в 2016 году технология распределенных реестров была признана одной из наиболее динамично развивающихся и перспективных [1]. Исследования теории развития информационного управления считают, что технологии распределенных реестров могут быть широко задействованы в будущих инновационных системах контроля и отчетности [2].

Предпринимаются попытки провести стандартизацию технологии, ее архитектуры и онтологии, определить требования к программно-аппаратным и программным средствам, а также регламентировать сферы применения технологии Блокчейн для широкого внедрения. Так, в Российской Федерации издан приказ Федерального агентства по техническому регулированию и метрологии от 15 декабря 2017 г. № 2831 «О создании технического комитета по стандартизации "Программно-аппаратные средства технологий распределенного реестра и Блокчейн"».

В Республике Беларусь «легализация» применения данной технологии определена Декретом № 8 Президента Республики Беларусь «О развитии цифровой экономики» [3].

В средствах массовой информации появилась и продолжает появляться информация о внедрении данной технологии, формируются бизнес-ассоциации, занимающиеся данной проблематикой.

Основная часть.

2. Основы для роста популярности технологии распределенных реестров. Для анализа возможностей применения технологии необходимо обозначить условия, определившие возникновение технологии распределенных реестров. Зарождение технологии связано с потребностями финансового рынка США и попытками оптимизировать схемы безденежных платежей с переводом финансовых транзакций в цифровую среду.

Учитывая бурный рост ИКТ в 1990-х годах и становление цифровой эпохи в указанный период, ненадежность работы популярного в то время криптографического алгоритма шифрования RSA и его низкую скорость работы, исследователи активно начали разработки в данном направлении и к 2000-м годам уже сформировались разнообразные подходы и технические решения, предназначенные для осуществления финансовых микротранзакций. Особо сильно исследователей интересовал вопрос анонимности микротранзакций ввиду роста популярности в начале 1990-х годов таких течений, как шифро-панк и крипто-анархизм [4] (из деятелей современности в данном направлении можно выделить Джулиана Пола Ассанжа, основателя известной международной некоммерческой организации WikiLeaks).

Исследователи выделили несколько групп решений возникших проблем [5]:

1. Онлайн решения, представленные в виде:

– банковских карт;

– систем анонимных микротранзакций на основе протокола NetBill;

– электронных денег DigiCash и NetCash, электронной чековой книжки NetCheque.

2. Решения на основе использования физических носителей и вычислительных мощностей, представленные в виде:

– электронных кошельков, представляющих собой защищенную смарт-карту с пополняемым пользователем балансом;

– системы микротранзакций MicroMint, фактически являющейся прообразом технологии распределенных реестров.

3. Решения на основе схемы подписки.

4. Решения на основе цифровых купонов — системы PayWord, NetCard, PayTree, micro-iKP.

5. Решения на основе вероятностных схем, предполагающие, что пользователь обозначает свои намерения по осуществлению транзакции, а момент ее завершения зависит от вычислительных мощностей и сформированной очереди намерений.

Предложенная модель группировки решений не является показательной в связи с тем, что окончательные технологические решения зачастую являются комбинированными и сочетают в себе элементы различных групп из перечисленных выше.

Среди ограничивающих факторов развития и распространения технологий в период их зарождения выделялись такие, как ограниченность в вычислительных мощностях серверов и низкий уровень развития ИКТ. В это же время стало известно об основных недостатках предложенных решений:

– потребность в наличии постоянного доступа к сети (следствие низкого уровня развития

ИКТ) (фактически проблемой являлось мошенничество с электронными платежами, в том числе схемы двойного использования электронных денег, превышение лимита средств на счету, при нахождении в режиме отсутствия подключения к сети и серверной инфраструктуре);

– потребность участия в «гонке вооружений» вычислительных мощностей для обеспечения масштабирования системы и, прежде всего, поддержания должного уровня информационной безопасности);

– отсутствие анонимности транзакций пользователей вопреки ожиданиям потребителей;

– низкая скорость транзакций;

– сложность построения системы;

– высокие затраты на обработку и хранение данных, в том числе высокая стоимость компьютерных вычислений, накопителей данных, высокие энергозатраты и необходимость создания специализированных центров обработки данных с повышенными требованиями к охлаждению вычислительного оборудования.

Ряд обозначенных проблем являются историческими и обусловлены тем, что идеи обогнали имеющиеся в наличии технологии, однако многие проблемы так и остались нерешенными.

3. Технология распределенных реестров. Рост популярности технологии распределенных реестров принято связывать с именем Сатоши Накамото, который в 2008 году опубликовал статью «Bitcoin: A Peer-to-Peer Electronic Cash System» [6].

Основная задача, решаемая предложенной технологией — создание механизма формирования реестра записей о транзакциях в условиях отсутствия доверительных отношений между участниками, т. е. создание журнала транзакций, из которого ни один участник не может удалить запись или подделать ее. Основным принципом доверенной среды является децентрализация хранения журнала и механизм гарантии его идентичности.

3.1. Основы решения. Фундаментом схемного решения, предложенного разработчиками Блокчейн, является ряд технологий, разработанных в период 1980–2000-х годов, среди которых наиболее важными являются:

1) анонимизация электронных платежей с отслеживанием состояния для предотвращения двойного использования электронных монет [7];

2) технология сопряженных меток времени транзакций для их формирования в связанные цепочки [8, 9, 10, 11], изначально разработанная для нотариального заверения деловой переписки и контрактов в цифровом виде;

3) технология построения структуры данных путем вычисления хэш-функций (дерево Меркла) на основе патента США №4309569, опубликованного 05.01.1982;

4) технология синхронизации состояния распределенной системы при обмене данными в недоверенной среде [12], которая была впервые предложена для защиты от спама, рассылаемого по электронной почте [13].

5) технология децентрализованного хранения и обмена данными посредством одноранговых (пиринговых) сетей.

3.2. MicroMint. В 1996 году авторами алгоритма шифрования RSA Р. Райвестом и А. Шамиром была опубликована работа «PayWord and MicroMint: two simple micropayment schemes» [14], определившая основные вопросы обеспечения безопасности инновационной системы микротранзакций и содержащая принципы функционирования 2-х различных по принципу работы систем осуществления финансовых транзакций.

Можно утверждать, что одна из двух платежных систем (MicroMint) является прародителем технологии, предложенной С. Накамото.

Основным отличием в этих системах является то, что «чеканку» электронных монет в системе MicroMint осуществляет так называемый брокер, фактически реальный банк, что не подрывает олигополию банковской системы, являющуюся естественным регулятором процесса «производства» денежной массы. В соответствии с предложенным решением генерация осуществляется в течение месяца для использования монет в последующем месяце. Пользователь приобретает электронные монеты у брокера и тратит их в сети Интернет. Продавец в течение дня возвращает электронный жетон брокеру в обмен на реальные деньги. В конце месяца происходит обнуление сгенерированной массы виртуальных монет.

Недостатком данной системы, не позволившим ей обрести популярность наследницы, является именно ориентирование на олигополию — на момент изобретения данного решения стоимость компьютерного оборудования была значительной и проект требовал больших инвестиций при распространении в то время глобальной идеи децентрализации и борьбы с засильем корпораций.

В начале 2000-х годов началась эпоха бурной компьютеризации, роста и доступности вычислительных мощностей. Вместе с тем, предложенная технология предполагала безоговорочное

вычислительное преимущество серверных мощностей брокеров, осуществляющих вычисление коллизий хэш-функции при генерации электронных монет. При невыполнении этого требования снижалась криптографическая стойкость системы [15].

3.3. Блокчейн Накамото. Предложенная Сатоши Накамото технология распределенных реестров, получившая впоследствии название «Блокчейн», сочетает в себе перечисленные выше решения, либо решения, полученные в результате их эволюционного развития. Однако наиболее значимым решением является изобретение механизма обеспечения работоспособности этой технологии.

На примере MicroMint уже был известен основной недостаток подобных систем — снижение с течением времени криптографической стойкости. Накамото удалось решить данную проблему, сохранив принцип обеспечения вычислительных мощностей брокерами, однако обеспечив такую возможность любому пользователю технологии, то есть фактически нарушив существовавшую веками банковскую олигополию.

Технология стала базироваться на соревновании между участниками и ориентировалась исключительно на общество потребления.

Механизм Блокчейн базируется на технологии защиты от спама и DOS-атак, которая предполагает осуществление ряда компьютерных вычислений, требующих гарантированных затрат некоторого неопределенного количества времени и ресурсов, превышающих суммарную выгоду от вероятных действий злоумышленника.

Изобретение Накамото предполагает, что данные вычисления направлены на обеспечение безопасности и поддержку работы всего реестра. Участники сети обмена данными распределенного реестра выполняют вычислительные задачи и первый участник, нашедший решение, получает право внести в реестр новые записи о транзакциях в виде отдельного блока цепочки. В обмен на использование вычислительных мощностей пользователя и затрачиваемые ресурсы, пользователь получает некоторое вознаграждение в виде так называемой криптовалюты.

3.4. Децентрализация системы. Основным принципом построения систем, использующих распределенные реестры, является децентрализация — абсолютное равноправие объединенных между собой электронно-вычислительных устройств, которые имеют равнозначные функции, и являются клиентом и сервером одновременно. Сети, работающие по такому принципу, называются одноранговыми или пиринговыми сетями и представляют собой равноправное объединение ЭВМ всех участников, называемых в таких системах пирами. От клиент-серверной архитектуры, которая легла в основу построения Интернета, такие сети отличаются непосредственно тем, что подобная организация способна сохранить работоспособность всей пиринговой сети при любом количестве доступных узлов, а также при любом их сочетании. То есть, при работе с обычными сетями все зависит от пропускной способности самого сервера, а в случае пиринговых сетей такого существенного недостатка нет.

Децентрализованная сеть на основе P2P-сетей обеспечивает естественное ограничение, определяющее информационную безопасность всего вычислительного объединения – ни один вычислительный кластер не должен иметь более 50 % вычислительной мощности.

4. Алгоритмы достижения консенсуса сети Блокчейн. В основе технологии Блокчейн лежит алгоритм достижения консенсуса в распределенной вычислительной сети.

Одним из способов достижения консенсуса является решение так называемой задачи византийских генералов для синхронизации состояния всех вычислительных узлов системы и приведения системы к общему знаменателю [12].

Первое практическое применение решения задачи византийских генералов Byzantine Fault Tolerance (BFT) заключалось в защите от спама, рассылаемого по электронной почте [13].

Схожий принцип был использован А. Бэком при разработке механизма защиты от спама на основе программного вычисления коллизий хэш-функции заданной сложности [16].

В 2002 году Бэком в статье «Hashcash — a denial of service counter-measure» для защиты от DOS-атак был предложен механизм, предполагающий использование особого криптографического жетона (token), генерируемого в результате проведения ряда вычислений и являющегося подтверждением проведенных криптографических вычислений (proof-of-work) [17].

Именно принцип Proof-of-Work (POW) и был использован при создании технологии Блокчейн в 2008 году [6].

Таким образом, на текущий момент в качестве алгоритмов достижения консенсуса блокчейн-платформами используются решения на базе BFT либо на базе POW.

4.1. Алгоритм POW. Принцип работы алгоритма с POW заключается в следующем: вычислительный кластер (вычислительный узел, отдельные вычислительные мощности участника гонки вычислений) вычисляет хэш-сумму всех блоков действительных транзакций, находящихся в состоянии ожидания подтверждения. Затем запускаются вычисления для нахождения хеш-кода в соответствии с установленными правилами Блокчейн-платформы в попытке сделать это раньше иных узлов. В случае успеха вычисленная хэш-сумма блока войдет в Блокчейн, а участники вычислительного узла получат вознаграждение в виде криптовалюты.

Вычислительные узлы, работающие с платформами на алгоритмах POW в качестве принципа достижения консенсуса, имеют значительное энергопотребление вне зависимости от результата — фактически узлы соревнуются в вычислительных мощностях и постоянно работают на предельных нагрузках, затрачивая электрическую энергию как на обеспечение вычислений, так и на удаление избытков тепловой энергии и охлаждение. В сети Bitcoin мировое годовое потребление электрической энергии превышает 40 ТВт·ч, что сравнимо с годовым потреблением Республики Беларусь — свыше 34 ТВт·ч [18].

Соревновательный характер извлечения прибыли участниками сети Блокчейн приводит к дополнительной проблеме алгоритма POW, которая заключается в создании крупных вычислительных кластеров с суммарной вычислительной мощностью, превышающей 51 % всех мощностей сети. Это дает им возможность добавлять новые блоки, манипулировать двусторонним операциями и не подтверждать новые транзакции, а также использовать одну и ту же криптомонету несколько раз.

4.2. Алгоритм PBFT. Алгоритм PBFT (Practical Byzantine Fault Tolerance) лег в основу алгоритмов консенсуса, используемых Hyperledger, Ripple, Stellar и Tendermint. PBFT представляет собой развитие теории, сформулированной в [12]. Практическое решение задачи достигается при условии, что более 1/3 вычислительных узлов — доверенные.

Использование алгоритма PBFT имеет ряд ограничений. Алгоритм работает только если все сообщения доставляются, хоть и с задержкой. Системы, построенные на алгоритме PBFT, имеют заранее определенных участников, осуществляющих чеканку виртуальных монет (в терминологии BFT — «генералов»).

Блокчейн-платформы, построенные на основе PBFT и их производных, относят к эксклюзивным Блокчейн-платформам (Permissioned, в противоположность децентрализованным — Permissionless).

4.3. Альтернативные алгоритмы консенсуса. Ввиду очевидных недостатков POW и централизованного принципа построения систем с PBFT, исследователями был разработан ряд альтернативных алгоритмов, например, POS (Proof-of-Stake, подтверждение доли участия). Алгоритм в целом схож с POW, однако узлы соревнуются не в вычислительной мощности, а в величине ставки криптовалюты на успешность будущих вычислений. Алгоритм значительно менее энергозатратный и является развитием алгоритма POW.

5. Недостатки технологии распределенных реестров. Технология распределенных реестров, как и технологические решения, на базе которых построен Блокчейн, имеет ряд недостатков. Часть из них имеет «врожденный» характер, часть обнаружилась при росте популярности и связана непосредственно с кризисом роста, часть связана с относительной новизной решений и множеством до конца не проанализированных моментов. Среди всех недостатков можно выделить один из важнейших — технология распределенных реестров является популярной платформой для реализации мошеннических схем, основанных на схеме Понци — финансовой инвестиционной пирамиде, которая предлагает потенциальным участникам осуществить инвестирование в проекты на базе Блокчейн-технологий.

5.1. Криптовалюта. В качестве опорной среды поддержки предложенного Накамото технологического решения используется существующая телекоммуникационная инфраструктура (сети связи) и децентрализованные аппаратно-вычислительные узлы участников. Это обеспечивает необходимую гибкость системы, ее масштабируемость и надежность. Разработчики ввели понятие «криптовалюта» как составляющую, определяющую интересы участников вычислительных узлов.

Таким образом, технология распределенных реестров базируется на эмиссии (чеканке или «майнинге») собственной псевдоплатежной виртуальной денежной массы и нежизнеспособна при отсутствии возможности конвертировать эмитированные виртуальные монеты в реальные финансовые средства, товары и услуги для

Таблица 1. Крупнейшие вычислительные узлы в сети участников распределенных реестров на базе криптовалюты Bitcoin по состоянию на 2018 год
Table 1. The largest computing nodes in the network of participants of distributed registries based on Bitcoin cryptocurrency (2018)

Наименование узла	Доля вычислительной мощности	Принадлежность
BTC.com	36,5 %	Китай
F2Pool	10,1 %	Китай
ViaBTC	9,4 %	Китай
BTC.TOP	7,5 %	Китай
AntPool	7,5 %	Китай
SlushPool	5,7 %	Чехия
Bixin	3,1 %	Китай
BitFury	3,1 %	Грузия
BitClub Network	1,9 %	Великобритания
BW.com	1,9 %	Китай
BTCC Pool	1,3 %	Китай

компенсации собственных затрат на поддержку телекоммуникационной инфраструктуры и связанных с ее эксплуатацией расходов.

Необходимо отметить, что разработчики Блокчейн-платформ ведут активную работу по поиску решения, позволяющего снизить зависимость от рядовых пользователей, обеспечивающих работу технологии (т. н. «майнеров»), фактически приводя систему к виду, предложенному Ривестом и Шамиром в MicroMint, с созданием крупных вычислительных узлов-брокеров.

Например, в вычислительной сети пользователей Ripple в обороте находятся централизованно «отчеканенные» цифровые монеты, которые используются для снижения стоимости транзакций в банковской сфере — фактически технология разработана по заказу банковской сферы для обеспечения ее потребностей.

5.2. Создание крупных вычислительных узлов. Для технологии распределенных реестров жизненно необходимо наличие мотивированных пользователей.

В соответствии с принципом работы технологии Блокчейн, рост количества блоков распределенного реестра приводит к повышению сложности вычислений и приводит к снижению эффективности чеканки криптовалют участниками, что снижает их персональную мотивацию.

Это привело к централизации участников и формированию крупных узлов вычислений за счет объединения в сообщества с четкими правилами и регламентами, а также управлением.

Крупнейшие вычислительные узлы в сети участников распределенных реестров на базе криптовалюты Bitcoin по состоянию на 2018 год приведены в таблице 1 (данные взяты с официальной страницы сайта www.bitcoin.com и доступны по ссылке https://news.bitcoin.com/the-anonymous-bitcoin-org-owner-accuses-btc-mining-pools-of-centralization/).

Крупнейшие вычислительные узлы в сети участников распределенных реестров на базе технологии Ethereum по состоянию на 2018 год приведены в таблице 2 (данные доступны по ссылке https://www.etherchain.org/charts/topMiners).

Понятие децентрализации применительно к технологии распределенных реестров носит скорее формальный характер — система напрямую зависит от влияния крупнейших игроков рынка, причем по состоянию на 2018 года Китай владеет не менее 70 % вычислительных мощностей из всех задействованных в технологии распределенных реестров.

5.3. Низкая скорость транзакций. Платформы на базе Блокчейн-технологии, создаваемые в противовес существующей банковской олигополии, прежде всего, как инструмент осуществления финансовых транзакций, имеют «врожденную» низкую скорость транзакций. Данные по основным решениями на базе технологии Блокчейн приведены в таблице 3.

Справочно: международная платежная система Visa имеет скорость обмена сообщениями 65000 сообщений в секунду (данные взяты из электронного документа, размещенном на официальной странице по ссылке https://usa.visa.com/dam/VCOM/download/corporate/media/visanet-technology/aboutvisafactsheet.pdf).

Таблица 2. Крупнейшие вычислительные узлы в сети участников распределенных реестров на базе технологии Ethereum по состоянию на 2018 год
Table 2. The largest computing nodes in the network of participants in distributed registries based on Ethereum technology (2018)

Наименование узла	Доля вычислительной мощности	Принадлежность
Ethermine	25,6 %	Австрия
Sparkpool	22,0 %	Китай
Nanopool	12,3 %	н/д
f2pool2	12,3 %	Китай
miningpoolhub1	8,9 %	н/д
DwarfPool1	1,9 %	Европа
uupool	1,7 %	н/д
bw	1,3%	Китай

Таблица 3. Данные по основным решениям на базе технологии Блокчейн
Table 3. Data on major solutions based on Blockchain technology

Наименование решений	Скорость, сообщений в секунду
Ripple	1500
Bitcoin Cash	60
Litecoin	56
Dash	48
Ethereum	20
Bitcoin	7

6. Варианты реализации технологии. По состоянию на 2018 год создано значительное количество альтернативных вариантов технологии Блокчейн: Namecoin, Emercoin, Ethereum, Bitnation, Hyperledger, EOS, IBM Blockchain, Multichain, NEM.

Альтернативные решения базируются на уникальных разработках, предназначенных для улучшения и расширения функционала сети, повышения ее безопасности и достижения консенсуса.

В среде разработчиков создание альтернативных решений Блокчейн имеет следующие направления:

– создание альтернативной платформы для реализации технологии Блокчейн;

– создание ответвления от «материнской» платформы, несовместимого с материнской платформой (возможно отсутствие поддержки новой платформой старых реестров и криптовалюты участников);

– создание ответвления от материнской платформы с поддержкой криптовалюты и базового реестра.

7. Предпосылки внедрения технологии.

7.1. Понятие степени готовности технологии. В соответствии с принятой практикой, внедрение технологических решений основывается на ряде необходимых предварительных процедур.

Ввиду бурного развития технологий в капиталистических странах во второй половине прошлого века возникла необходимость внедрения основных принципов оценки «зрелости» технологии до ее широкого использования.

С этой целью впервые в 1974 году специалистом Национального управления по аэронавтике и исследованию космического пространства (NASA) была предложена классификация, опирающая на стадию разработки технологии. В дальнейшем классификация готовности технологии (Technology Readiness Level) была уточнена, в том числе для ее использования при описании процессов, связанных с программированием, и стала включать девять уровней TRL1–TRL9. По предложенной классификации стадия TRL1 — технология, представленная в виде описания основных принципов; TRL9 — технология, прошедшая испытания, имеющая сопроводительную документацию и готовая к промышленному применению.

Данная классификация получила широкое распространение, в том числе используется при оценке проектов рамочной программы Европейского союза по развитию научных исследований и технологий «Горизонт 2020».

В отношении технологии распределенных реестров можно утверждать, что весь необходимый комплекс разработки, испытаний

и нормативно-правового регулирования, позволяющий рассматривать внедрение технологии в секторах государственного управления, не был осуществлен. Положительный мировой опыт внедрения относится к коммерческому использованию.

Степень готовности технологии по предложенной NASA классификации можно оценить, как TRL7. Данный уровень характеризуется следующим образом: разработан прототип программного обеспечения, обладающий основными функциями, необходимыми для демонстрации и тестирования; технологические решения интегрируются с операционными аппаратными/программными системами, демонстрируют операционную осуществимость; устранено большинство программных ошибок; доступна ограниченная документация.

7.2. Цикл зрелости технологии. Американский исследователь Рой Амара провел эмпирическое наблюдение и сформулировал закон, впоследствии названный «Закон Амары»: «Мы склонны переоценивать эффект технологии в короткой перспективе и недооценивать в длинной», предсказав кризис 2000 года в сфере IT-индустрии.

Наибольший вклад в описание процессов создания новых технологий внесла исследовательская компания Gartner. Взяв за основу кривую циклов Н. Д. Кондратьева, предложенную в работе 1925 года «Длинные волны конъюнктуры» и кривую «взросления» технологии, исследователи из Гарварда в 1995 году была вывели эмпирическую «кривую Гартнера» — кривую зрелости технологии, графически представляющую стадии, через которые проходит технологическое новшество в современном мире в ходе своего становления (рис. 1) [19].

В отношении технологии распределенных реестров можно сказать, что по кривой Гартнера она находится в стадии пика завышенных ожиданий (Peak of Inflated Expectations).

В отношении технологии распределенных реестров кривая Гартнера демонстрирует текущее состояние как этап негативных отзывов в прессе и свидетельствует об общем снижении интереса к технологии на фоне падения курсов криптовалют. Стоит ожидать снижение заинтересованности технологией частными инвесторами на фоне повышения интереса корпоративного сектора и сектора государственного управления ввиду новых перспектив технологии за счет использования новых алгоритмов и возможностей технологии.

8. Текущее состояние технологии. Высокая, но не окончательная степень готовности технологии объясняется постоянной работой исследователей над оптимизацией технологии

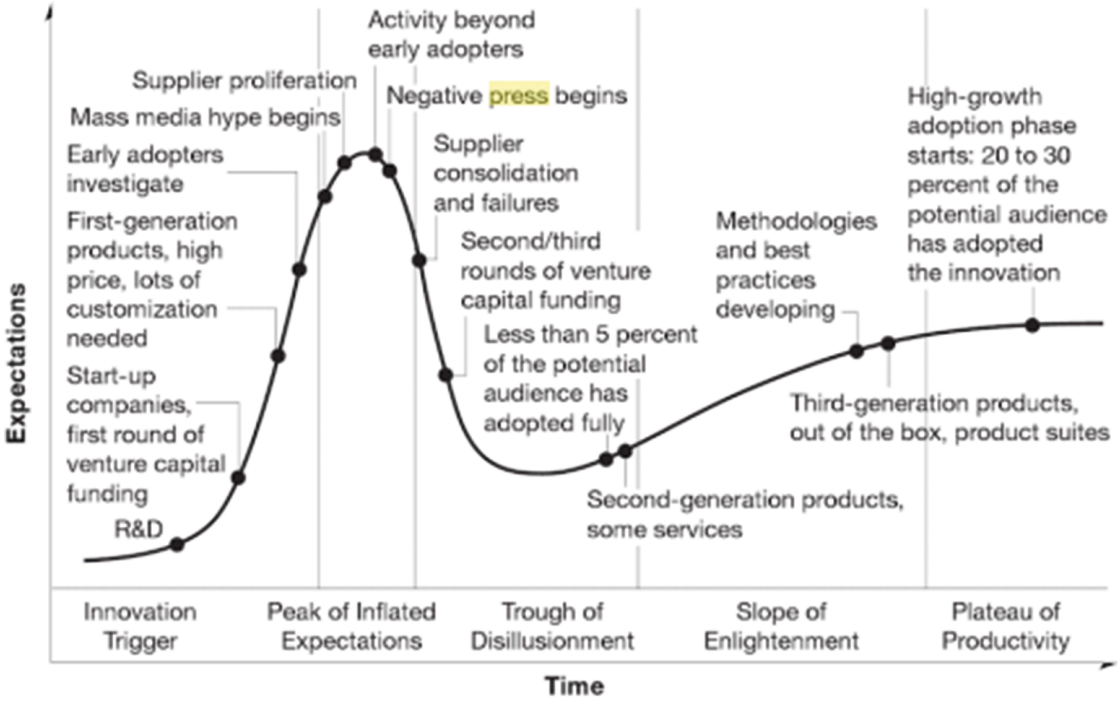

Рис. 1. Кривая Гартнера
Fig. 1. Gartner graph

распределенных реестров и работой над устранением недостатков.

Это выражается прежде всего в изменении алгоритма достижения консенсуса в сети пользователей — разработчики Блокчейн-платформ либо осуществляют, либо планируют переход от алгоритмов POW к более совершенным, не имеющим недостатков базового решения (таких как чрезмерное энергопотребление, масштабируемость системы и низкая скорость транзакций).

Другим фактором является постепенный уход от сложившейся модели чеканки электронных монет рядовыми участниками. Криптовалюты чрезвычайно волатильны — курс обмена нестабилен и меняется в значительной степени за кратчайшие промежутки времени. Блокчейн-платформа, построенная на алгоритмах базового решения, зависит от финансовой мотивации участников, ввиду чего есть угрозы работоспособности всей системы.

Кроме того, осуществляется постепенный переход от Permissionless к Permissioned блокчейн-платформам, в неявной форме за счет формирования крупных вычислительных узлов и в явной форме за счет использования конкретных технических решений.

9. Перспективы применения технологии в системе образования. Перспективным направлением практического использования технологии Блокчейн являются так называемые «умные контракты» (смарт-контракты). Удобство заключается в создании единой платформы для установления договорных отношений как в рамках государства, так и на межгосударственном уровне при наличии соответствующей законодательной базы, в том числе за счет значительного сокращения сроков подписания. В таком случае Блокчейн-платформа будет содержать данные о смарт-контрактах, однако необходимо разрабатывать подробные алгоритмы взаимодействия участников смарт-контрактов для подтверждения не только факта принятия соглашения всеми сторонами, но и подтверждения выполнения условий всеми сторонами в установленные сроки.

Технология Блокчейн позволяет создавать реестры записей оказанных электронных услуг, осуществляемых автоматизированными системами по запросам пользователей. Реестры блоков могут содержать данные о перечнях услуг, запросах об оказании и сведения об оплате услуг и результаты оказания/неоказания услуг.

Внедрение технологии Блокчейн в систему ведомственного документооборота повысит достоверность передачи данных, улучшит контроль исполнения поручений, позволит отслеживать отдельные этапы исполнения поручений, а также реализации отдельных проектов и программ, включающих значительное число этапов и задач.

Актуальной задачей, решаемой с помощью Блокчейн, может стать оптимизация деятельности учреждений образования всех уровней по приему обучающихся, включая регистрацию поданных документов, фиксацию приема заявок, их одобрение и отклонение, прогресс обучающихся, а также данные о документах об образовании.

Кроме указанного Блокчейн может применяться для решения вопросов, касающихся лицензирования образовательных услуг. С использованием технологии Блокчейн также может осуществляться защита авторских прав образовательных материалов при внедрении хэш-кода в программные образовательные продукты, содержащие информацию об авторстве.

10. Шаги для внедрения Блокчейн. Необходимым шагом для широкого внедрения технологии является доработка технологии до уровня готовности, соответствующего национальным требованиям законодательства, включая единый стандарт и терминологию, используемую при описании алгоритмов и решений.

Дополнительно необходима легализация деятельности по обороту криптовалют и создание национальной биржи, оказывающей услуги, связанные с обменом криптовалют.

Заключение. Технология Блокчейн — одно из последних достижений ИКТ-индустрии, формирующее новую парадигму взаимоотношений между пользователями и новые шаблоны бизнес-процессов.

Эволюция технологии распределённых реестров привела к созданию решений, имеющих высокую степень готовности к применению, и в настоящее время находит применение в банковской сфере в части оптимизации расходов на финансовые транзакции.

Технология распределённых реестров может быть использована в системе образования как гибкий и экономически эффективный инструмент обмена данными в вопросах лицензирования деятельности учреждений образования, подтверждения подлинности выданных документов об образовании, оказания образовательных услуг. Блокчейн может применяться как альтернативный способ осуществления микрофинансовых

транзакций, осуществляемых в учреждениях образования.

В целом, использование технологии Блокчейн позволяет создавать образовательные технологии, сервисы и обеспечивать оказание услуг минуя традиционно сформировавшиеся схемы, с участием большого числа посредников, что приведёт к значительному снижению стоимости транзакций.

Необходимо отметить, что применение технологии распределенных реестров требует предварительного решения вопросов, связанных с разработкой нормативного регулирования и методического обеспечения использования и непосредственной адаптации технологических решений под решение конкретных отраслевых задач.

Список литературы

1. Top 10 Emerging Technologies of 2016. Global Agenda: World Economic Forum / Meta-Council on Emerging Technologies; ed. B. Meyerson. – Geneva, 2016. – Mode of access: http://www3.weforum.org/docs/GAC16_Top10_Emerging_Technologies_2016_report.pdf. – Date of access: 05.12.2018.
2. Вишняков, В. Использование интеллектуальных и блокчейн технологий в информационном управлении / В. Вишняков // Системный анализ и прикладная информатика [Электронный ресурс]. –2018, №1. – Режим доступа: https://cyberleninka.ru/article/n/ispolzovanie-intellektualnyh-i-blokcheyn-tehnologiy-v-informatsionnom-upravlenii. – Дата доступа: 05.12.2018.
3. О нормативных правовых актах Республики Беларусь: Декрет Президента Республики Беларусь от 21 декабря 2017 г. № 8: с прилож: текст по состоянию на 5 декабря 2018 г. // Официальный интер-нет-портал Президента Республики Беларусь. – Режим доступа: http://president.gov.by/ru/official_documents_ru/view/dekret-8-ot-21-dekabrja-2017-g-17716/. – Дата доступа: 05.12.2018.
4. Timothy C. May The Crypto Anarchist Manifesto / Timothy C. May [Electronic resource]. – 1992. – Mode of access: https://www.activism.net/cypherpunk/crypto-anarchy.html. – Date of access: 05.12.2018.
5. Lipton, R. J. Micro-payments via efficient coin-flipping / R. J. Lipton, R. Ostrovsky // International Confer-ence on Financial Cryptography and Data Security: Lecture Notes in Computer Science, Anguilla, 23–25 Feb-ruary, 1998 / Springer; ed. R. Hirchfeld. – Berlin, Heidelberg, 1998. – Vol. 1465. – Mode of access: https://link.springer.com/chapter/10.1007/BFb0055469. – Date of access: 05.12.2018.
6. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System / Satoshi Nakamoto // [Electronic resource]. – 2008. – Mode of access: https://bitcoin.org/bitcoin.pdf. – Date of access: 05.12.2018.
7. Chaum, D. Untraceable Electronic Cash / D. Chaum, A. Fiat, M. Naor // Conference Advances in Cryptol-ogy – CRYPTO' 88: Lecture Notes in Computer Science, 1988 / Springer; ed. S. Goldwasser. – New York, 1988. – Pp. 319–327. – Mode of access: https://link.springer.com/chapter/10.1007/0-387-34799-2_25. – Date of access: 05.12.2018.
8. Massias, H. Design of a secure timestamping service with minimal trust require-ments / H. Massias, X. S. Avila, J. J. Quisquater // 20th Symposium on Information Theory in the Benelux, May, 1999 / Werkgemeen-schaft voor Informatie en Communicatietheorie, Enschede; ed. Barbé A. – 1999. – Pp. 79–86. – Mode of ac-cess: https://uclouvain.be/crypto/services/download/publications.pdf.9ca0971b29e9c614.7064663131332e706466.pdf. – Date of access: 05.12.18.
9. Haber, S. How to time-stamp a digital document / S. Haber, W.S. Stornetta // Journal of Cryptology. – 1991. – Vol. 3, issue 2. – Pp. 99–111. – Mode of access: https://link.springer.com/article/10.1007/BF00196791. – Date of access: 05.12.2018.
10. Bayer, D. Improving the efficiency and reliability of digital time-stamping / D. Bayer, S. Haber, W. S. Stornetta // Sequences II Methods in Communication, Security and Computer Science / Springer-Verlag; ed. R. Capocelli. – New York, 1993. – Pp. 329–334. – Mode of access: https://link.springer.com/chapter/10.1007/978-1-4613-9323-8_24. – Date of access: 05.12.2018.
11. Haber, S. Secure names for bit-strings / S. Haber, W. S. Stornetta // Proceedings of the 4th ACM confer-ence on Computer and communications security, Zurich, 1–4 April, 1997 / ACM; ed. Graveman R.F., – New York, 1997. – Pp. 28–35. – Mode of access: https://dl.acm.org/citation.cfm?doid=266420.266430. – Date of access: 05.12.2018.
12. Lamport, L. The Byzantine Generals Problem / L. Lamport, R. Shostak, M. Pease // ACM Transactions on Programming Languages and Systems (TOPLAS). – 1982. – Vol. 4, issue 3. – Pp. 382–401. – Mode of ac-cess: https://dl.acm.org/citation.cfm?id=357176. – Date of access: 05.12.2018.
13. Dwork, C. Pricing via Processing or Combatting Junk Mail / C. Dwork, M. Naor // Conference Advances in Cryptology – CRYPTO' 92: Lecture Notes in Computer Science, Santa Barbara, 16-20 August 1992 / Springer; ed. E. F. Brickell. – Berlin: Heidelberg, 1992. – Pp. 139–147. – Mode of access https://link.springer.com/chapter/10.1007/3-540-48071-4_10. – Date of access: 05.12.2018.
14. Rivest, R. L. PayWord and MicroMint: two simple micropayment schemes / R. L. Rivest, A. Shamir // Se-curity Protocols: International Workshop on Security Protocols: Lecture Notes in Computer Science, Cam-bridge, 10-12 April 1996 / Cambridge; ed. M. Lomas. – Berlin: Heidelberg, 1996. – Pp. 69–87. – Mode of ac-cess: https://link.springer.com/

chapter/10.1007/3-540-62494-5_6. – Date of access: 05.12.2018.
15. Van Someren, N. The Practical Problems of Implementing MicroMint / N. Van Someren // 5th International Conference on Financial Cryptography FC 2001: Lecture Notes in Computer Science, Grand Cayman, 19-22 February 2001 / Springer; ed. P. Syverson. – Berlin, Heidelberg, 2002. – Pp. 41–50. – Mode of access: https://link.springer.com/chapter/10.1007/3-540-46088-8_3. – Date of access: 05.12.2018.
16. Back, A. Hash cash postage implementation / A. Back // hashcash.org [Electronic resource]. – 1997. – Mode of access: http://www.hashcash.org/papers/announce.txt. – Date of access: 05.12.2018.
17. Back, A. Hashcash - a denial of service counter-measure / A. Back // hashcash.org [Electronic resource]. – 2002. – Mode of access: http://www.hashcash.org/hashcash.pdf. – Date of access: 05.12.2018.
18. Энергетика. Баланс электрической энергии // Национальный статистический комитет Республи-ки Беларусь [Электронный ресурс]. – 2018. – Режим доступа: http://www.belstat.gov.by/upload-belstat/upload-belstat-excel/Oficial_statistika/year-ru-energy-2018-01.xlsx. – Дата доступа: 05.12.2018.
19. Fenn, J. Mastering the Hype Cycle: How to Choose the Right Innovation at the Right Time / J. Fenn, M. Raskino // Gartner, Inc. – Harvard Business Press, 2008. – P. 67. – Mode of access: https://books.google.by/books/about/Mastering_the_Hype_Cycle.html?id=hOBMBmcmROAC&redir_esc=y. – Date of access: 05.12.2018.

References

1. Top 10 Emerging Technologies of 2016. Global Agenda: World Economic Forum. Geneva, 2016. Available at: http://www3.weforum.org/docs/GAC16_Top10_Emerging_Technologies_2016_report.pdf (accessed: 05.12.2018).
2. Vishnjakov V. The use of intelligent and blockchain technologies in information management. Sistemnyj analiz i prikladnaja informatika [System analysis and applied informatics], 2018, no. 1. Available at: https://cyberleninka.ru/article/n/ispolzovanie-intellektualnyh-i-blokcheyn-tehnologiy-v-informatsionnom-upravlenii. (accessed: 05.12.2018) (in Russian).
3. O normativnyh pravovyh aktah Respubliki Belarus': Dekret Prezidenta Respubliki Belarus' ot 21 dekabrja 2017 g. № 8: s prilozh: tekst po sostojaniju na 05 dekabrja 2018 g. [On normative legal acts of the Republic of Belarus: Decree of the President of the Republic of Belarus of December 21, 2017 No. 8: s appended: text as of December 5, 2018]. Available at: http://president.gov.by/ru/official_documents_ru/view/dekret-8-ot-21-dekabrja-2017-g-17716/ (accessed: 05.12.2018) (in Russian).
4. Timothy C. May The Crypto Anarchist Manifesto. Available at: https://www.activism.net/cypherpunk/crypto-anarchy.html (accessed: 05.12.2018) (in Russian).
5. Lipton R. J., Ostrovsky R. Micro-payments via efficient coin-flipping. International Conference on Financial Cryptography and Data Security: Lecture Notes in Computer Science, Anguilla, 23–25 February, 1998. Berlin: Heidelberg, 1998. Vol. 1465. Available at: https://link.springer.com/chapter/10.1007/BFb0055469 (accessed: 05.12.2018).
6. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available at: https://bitcoin.org/bitcoin.pdf (accessed: 05.12.2018).
7. Chaum D., Fiat A., Naor M. Untraceable Electronic Cash. Conference Advances in Cryptology – CRYP-TO' 88: Lecture Notes in Computer Science. New York, 1988, pp. 319–327. Available at: https://link.springer.com/chapter/10.1007/0-387-34799-2_25 (accessed: 05.12.2018).
8. Massias H., Avila X. S., Quisquater J. J. Design of a secure timestamping service with minimal trust require-ments. 20th Symposium on Information Theory in the Benelux, May, 1999, pp. 79–86. Available at: https://uclouvain.be/crypto/services/download/publications.pdf.9ca0971b29e9c614.7064663131332e706466.pdf (accessed: 05.12.2018).
9. Haber S., Stornetta W. S. How to time-stamp a digital document. Journal of Cryptology. 1991, vol. 3, issue 2, pp. 99–111. Available at: https://link.springer.com/article/10.1007/BF00196791 (accessed: 05.12.2018).
10. Bayer D., Haber S., Stornetta W. S. Improving the efficiency and reliability of digital time-stamping. Se-quences II Methods in Communication, Security and Computer Science. New York, 1993, pp. 329–334. Available at: https://link.springer.com/chapter/10.1007/978-1-4613-9323-8_24 (accessed: 05.12.2018).
11. Haber S., Stornetta W. S. Secure names for bit-strings. Proceedings of the 4th ACM conference on Com-puter and communications security, Zurich, 1–4 April, 1997. New York, 1997, pp. 28–35. Available at: https://dl.acm.org/citation.cfm?doid=266420.266430 (accessed: 05.12.2018).
12. Lamport L., Shostak R., Pease M. The Byzantine Generals Problem. ACM Transactions on Programming Languages and Systems (TOPLAS), 1982, vol. 4, issue 3, pp. 382–401. Available at: https://dl.acm.org/citation.cfm?id=357176 (accessed: 05.12.2018).
13. Dwork C., Naor M. Pricing via Processing or Combatting Junk Mail. Conference Advances in Cryptology – CRYPTO' 92: Lecture Notes in Computer Science, Santa Barbara, 16-20 August 1992. Berlin: Heidelberg, 1992, pp. 139–147. Available at: https://link.springer.com/chapter/10.1007/3-540-48071-4_10 (accessed: 05.12.2018).
14. Rivest R. L., Shamir A. PayWord and MicroMint: two simple micropayment schemes. Security Protocols: International Workshop on Security Protocols: Lecture Notes in Computer Science, Cambridge, 10-12 April 1996. Berlin: Heidelberg, 1996, pp. 69–87. Available at: https://link.springer.com/chapter/10.1007/3-540-62494-5_6 (accessed: 05.12.2018).

15. Van Someren N. The Practical Problems of Implementing MicroMint. 5th International Conference on Fi-nancial Cryptography FC 2001: Lecture Notes in Computer Science, Grand Cayman, 19-22 February 2001. Berlin: Heidelberg, 2002, pp. 41–50. Available at: https://link.springer.com/chapter/10.1007/3-540-46088-8_3 (accessed: 05.12.2018).
16. Back A. Hash cash postage implementation. Available at: http://www.hashcash.org/papers/announce.txt (accessed: 05.12.2018).
17. Back A. Hashcash — a denial of service counter-measure. Available at: http://www.hashcash.org/hashcash.pdf (accessed: 05.12.2018).
18. Jenergetika. Balans jelektricheskoj jenergii [Energy. Electric power balance]. Available at: http://www.belstat.gov.by/upload-belstat/upload-belstat-excel/Oficial_statistika/year-ru-energy-2018-01.xlsx (accessed: 05.12.2018) (in Russian).
19. Fenn J., Raskin M. Mastering the Hype Cycle: How to Choose the Right Innovation at the Right Time. Harvard Business Press, 2008, p. 67. Available at: https://books.google.by/books/about/Mastering_the_Hype_Cycle.html?id=hOBMBmcmROAC&redir_esc=y (accessed: 05.12.2018).

Received: 19.12.2018 *Поступила: 19.12.2018*