Торайғыров университетінің
ҒЫЛЫМИ ЖУРНАЛ

НАУЧНЫЙ ЖУРНАЛ
Торайгыров университета

ТОРАЙҒЫРОВ УНИВЕРСИТЕТІНІҢ ХАБАРШЫСЫ

Физика, математика және компьютерлік ғылымдар сериясы
1997 жылдан бастап шығады

TORAIGHYROV UNIVERSITY

ВЕСТНИК ТОРАЙГЫРОВ УНИВЕРСИТЕТА

Серия: Физика, математика и компьютерные науки
Издается с 1997 года

ISSN 2959-068X

№ 4 (2022)
Павлодар

НАУЧНЫЙ ЖУРНАЛ
ТОРАЙГЫРОВ УНИВЕРСИТЕТА

Серия: Физика, математика и компьютерные науки
выходит 4 раза в год

СВИДЕТЕЛЬСТВО
о постановке на переучет периодического печатного издания,
информационного агентства и сетевого издания
№ KZ91VPY00046988
выдано
Министерством информации и общественного развития
Республики Казахстан

Тематическая направленность
публикация материалов в области физики, математики,
механики и информатики

Подписной индекс – 76208

https://doi.org/ 10.48081/QTXQ7157

МРНТИ 06.73.45

https://doi.org// 10.48081/AFBS9207

О. Г. Потапенко[1], *А. О. Потапенко[2], А. О. Юсупова[3]
[1,2,3]Торайгыров университет, Республика Казахстан, г. Павлодар

АНАЛИЗ ОСНОВОПОЛАГАЮЩИХ ИССЛЕДОВАНИЙ ТЕХНОЛОГИИ БЛОКЧЕЙН

Чаще всего при транзакции денег или чего-либо ценного, люди и предприятия в значительной степени полагаются на посредников, таких как банки и правительство, чтобы обеспечить доверие и уверенность. Посредники выполняют ряд важных задач, которые помогают укрепить доверие в процессе транзакции, например, аутентификация и ведение записей. На сегодняшний день имеется возможность отправлять кому-то деньги напрямую без помощи банка – за секунды, а не дни, не платя банковские сборы. Есть возможность хранить деньги в онлайн-кошельке, не привязанном к банку, что означает, что только пользователь, создавший этот кошелек, имеет полный контроль над своими деньгами. Это лишь некоторые из важных вариантов использования технологии блокчейна. Тем не менее, для многих она по-прежнему остается незнакомой, некоторые не уверены в том, что она будет использоваться в будущем. Скептицизм, вокруг данной технологии понятен, потому что блокчейн еще находится на ранней стадии разработки и широкого внедрения. В статье сделана попытка рассмотрения основополагающих фундаментальных исследований на основе которых была построена технология блокчейн.

Ключевые слова: блокчейн, биткойн, хэширование, деревья Меркла, доказательство работы.

Введение

Исследования цифровой наличности за несколько десятилетий, начиная с 10-летнего Дэвида Чаума [1], не привел к коммерческому успеху, потому что для этого требовался централизованный банковский сервер, контролирующий систему, и ни один банк не хотел реализовывать данную идею. Вслед за этим появился биткойн, радикально отличающееся предложение для децентрализованной криптовалюты, которая не нуждалась в банках, и цифровая наличность, наконец, добилась успеха. Считается,

что изобретателем биткоина является Сатоши Накамото, а предложенный им биткойн не имеет ничего общего с более ранними академическими предложениями, однако, как показывает приведенный в статье анализ, почти все технические компоненты биткойна возникли в академической литературе 1980-х и 90-х годов. Это не умаляет достижений Накамото, а указывает на то, что в его разработке использовались более ранние фундаментальные исследования. Истинный прорыв Накамото – специфический, сложный способ соединения основных компонентов. Это помогает объяснить, почему биткойн был изобретен намного позже. Интеллектуальная история Биткойна также служит кейсом, демонстрирующим отношения между академическими кругами, внешними исследователями и практиками.

Материалы и методы

Идея бухгалтерской книги является отправной точкой для понимания биткойна. Это место для записи всех транзакций, происходящих в системе, оно открыто для всех участников системы и пользуется доверием. Биткойн конвертирует эту систему записи платежей в валюту. Транзакция имеет ценность по своей сути. Реестр должен быть неизменным или, точнее, только добавляться: должна быть возможность добавлять новые транзакции, но не удалять, изменять или переупорядочивать существующие. Также должен быть способ получить краткий криптографический дайджест состояния реестра в любой момент. Дайджест – это короткая строка, которая позволяет избежать хранения всего реестра, зная, что, если реестр будет каким-либо образом подделан, результирующий дайджест изменится, и, таким образом, фальсификация будет обнаружена. Причина этих свойств заключается в том, что в отличие от обычной структуры данных, которая хранится на одном компьютере, реестр представляет собой глобальную структуру данных, коллективно поддерживаемую группой взаимно не доверяющих друг другу участников. Это контрастирует с другим подходом к децентрализации цифровых реестров [2–4], в котором многие участники ведут локальные реестры, и пользователь, запрашивающий этот набор реестров, должен разрешать любые конфликты.

Структура данных реестра Биткойн заимствована с минимальными изменениями из серии статей Стюарта Хабера и Скотта Сторнетты, написанных между 1990 и 1997 годами (в их статье 1991 года был еще один соавтор, Дэйв Байер) [5–7]. Накамото говорит об этом в своем официальном документе о биткойнах [8]. Работа Хабера и Сторнетты была направлена на решение проблемы временных меток документов – они стремились создать службу «цифрового нотариуса». Для патентов, деловых контрактов и других документов может потребоваться установить, что документ был создан в определенный момент времени, а не позже. Их понятие документа

является довольно общим и может быть любым типом данных. Они вскользь упоминают о финансовых транзакциях как о потенциальном приложении, но это не было их целью.

В упрощенной версии предложения Хабера и Сторнетты документы постоянно создаются и транслируются. Создатель каждого документа утверждает время создания и подписывает документ, его метку времени и ранее переданный документ. Этот предыдущий документ подписал своего собственного предшественника, поэтому документы образуют длинную цепочку с указателями назад во времени. Внешний пользователь не может изменить сообщение с отметкой времени, поскольку оно подписано создателем, а создатель не может изменить сообщение, не изменив при этом всю цепочку последующих сообщений. Таким образом, если вам предоставляется один элемент в цепочке из надежного источника (например, другого пользователя или специализированной службы временных меток), вся цепочка до этого момента заблокирована, неизменяема и упорядочена во времени. В дальнейшем, если вы предполагаете, что система отклоняет документы с неправильным временем создания, вы можете быть разумно уверены, что документы по крайней мере настолько стары, насколько они заявлены. В любом случае, биткойн заимствует только структуру данных из работы Хабера и Сторнетты и реконструирует свои свойства безопасности, добавляя схему доказательства работы, описанную далее в этой статье.

В своих последующих статьях Хабер и Сторнетта представили другие идеи, которые делают эту структуру данных более эффективной и действенной (на некоторые из них намекали в их первой статье). Во-первых, ссылки между документами можно создавать с помощью хэшей, а не подписей; хэши проще и быстрее вычислять. Такие ссылки называются хэш-указателями. Во-вторых, вместо разделения документов по отдельности – что может быть неэффективно, если много документов создается примерно в одно и то же время – их можно сгруппировать в пакеты или блоки, при этом документы в каждом блоке будут иметь практически одинаковую отметку времени. В-третьих, внутри каждого блока документы могут быть связаны друг с другом бинарным деревом хэш-указателей, называемым деревом Меркла, а не линейной цепочкой. Между прочим, Джош Бенало и Майкл де Мар независимо друг от друга представили все три идеи в 1991 году [9], вскоре после выхода первой статьи Хабера и Сторнетты.

В дереве Меркла каждого блока листовые узлы являются транзакциями, и каждый внутренний узел по существу состоит из двух указателей. Эта структура данных имеет два важных свойства. Во-первых, хэш последнего блока действует как дайджест. Изменение любой из транзакций (листовых узлов) потребует распространения изменений на весь путь до корня блока и

корней всех последующих блоков. Таким образом, если вы знаете последний хэш, вы можете загрузить остальную часть реестра из ненадежного источника и убедиться, что он не изменился. Аналогичный аргумент устанавливает еще одно важное свойство структуры данных, то есть кто-то может эффективно доказать вам, что конкретная транзакция включена в реестр. Этот пользователь должен будет отправить вам только небольшое количество узлов в блоке этой транзакции (это точка дерева Меркла), а также небольшое количество информации для каждого следующего блока. Возможность эффективно подтверждать включение транзакций очень важна для производительности и масштабируемости. Деревья Меркла названы в честь Ральфа Меркла, пионера асимметричной криптографии, который предложил эту идею в своей статье 1980 года [10]. Его предполагаемое применение состояло в том, чтобы создать дайджест для общедоступного каталога цифровых сертификатов. Например, когда веб-сайт предоставляет вам сертификат, он также может предоставить краткое подтверждение того, что сертификат находится в глобальном каталоге. Вы можете эффективно проверить доказательство, если знаете корневой хэш дерева Меркла сертификатов в каталоге. Эта идея достаточно старая по криптографическим стандартам, но ее силу оценили только в последнее время. Она лежит в основе недавно внедренной системы прозрачности сертификатов [11]. В документе 2015 года предлагается CONIKS, который применяет идею к каталогам открытых ключей для сквозных зашифрованных электронных писем [12]. Эффективная проверка частей глобального состояния – одна из ключевых функций, предоставляемых реестром в Эфириуме, новой криптовалюте.

Биткойн может быть самым известным воплощением структур данных Хабера и Сторнетты в реальном мире, но не первым. По крайней мере две компании – Surety, основанная в середине 90-х годов, и Guardtime, основанная в 2007 году, – предлагают услуги по временной отметке документов. В обеих этих службах присутствует идея, упомянутая Байером, Хабером и Сторнеттой [5], которая заключается в периодической публикации корней Меркла в газете путем размещения рекламы.

Конечно, требования к интернет-валюте без центрального органа более жесткие. Распределенный реестр неизбежно будет иметь разветвления, что означает, что некоторые узлы будут думать, что блок A является последним блоком, в то время как другие узлы будут думать, что это блок B. Это может быть из-за злоумышленника, пытающегося нарушить работу реестра, или просто из-за сети. задержка, в результате чего блоки иногда генерируются почти одновременно разными узлами, не знающими о блоках друг друга. Одной связанной временной метки недостаточно для разрешения разветвлений, как показал Майк Джаст в 1998 году [13].

Другая область исследований, отказоустойчивые распределенные вычисления, изучала эту проблему, где она носит разные названия, включая репликацию состояния. Решением этой проблемы является такое, которое позволяет набору узлов применять одни и те же переходы состояний в одном и том же порядке — как правило, точный порядок не имеет значения, важно только, чтобы все узлы были согласованы. Для цифровой валюты реплицируемое состояние — это набор балансов, а транзакции — это переходы между состояниями. Ранние решения, в том числе Paxos, предложенные лауреатом премии Тьюринга Лесли Лэмпорт в 1989 г.[14, 15], рассмотрите репликацию состояния, когда каналы связи ненадежны и когда меньшинство узлов может демонстрировать определенные «реальные» сбои, такие как отключение навсегда или перезагрузка и отправка устаревших сообщений с момента первого отключения. За этим последовала обширная литература с более неблагоприятными условиями и компромиссами в эффективности.

Связанное направление работы изучало ситуацию, когда сеть в основном надежна (сообщения доставляются с ограниченной задержкой), но где определение «сбоя» было расширено для обработки любого отклонения от протокола. Такие византийские ошибки включают в себя как естественные ошибки, так и злонамеренное поведение. Впервые они были изучены в статье Лэмпорта, написанной в соавторстве с Робертом Шостаком и Маршаллом Пизом, еще в 1982 г [16]. Значительно позже, в 1999 г., знаковая статья Мигеля Кастро и Барбары Лисков представила PBFT (практическая византийская отказоустойчивость), которая вмещал как византийские ошибки, так и ненадежную сеть [17]. По сравнению со связанными временными метками литература по отказоустойчивости огромна и включает сотни вариантов и оптимизаций Paxos, PBFT и других основополагающих протоколов.

В своем оригинальном официальном документе Накамото не цитирует эту литературу и не использует ее язык. Он использует некоторые понятия, называя свой протокол механизмом консенсуса и рассматривая ошибки как в виде атакующих, так и в виде узлов, присоединяющихся к сети и покидающих ее. Это контрастирует с его явной зависимостью от литературы в связанных временных метках (и доказательстве работы, обсуждаемом далее). Отвечая на вопрос в списке рассылки об отношении Биткойна к проблеме византийских генералов (мысленный эксперимент, требующий решения BFT), Накамото утверждает, что цепочка доказательства работы решает эту проблему[18].

В последующие годы другие ученые изучали консенсус Накамото с точки зрения распределенных систем. Эта работа еще не завершена. Некоторые показывают, что свойства биткойна довольно слабые [19], в то время как другие утверждают, что точка зрения BFT не отражает свойства

согласованности биткойна [20]. Другой подход заключается в том, чтобы определить варианты хорошо изученных свойств и доказать, что биткойн им удовлетворяет [21]. Недавно эти определения были существенно уточнены, чтобы обеспечить более стандартное определение согласованности, которое выполняется при более реалистичных предположениях о доставке сообщений [22].Однако во всей этой работе делаются предположения о «честном», т. е. соответствующем протоколу, поведении среди подмножества участников, в то время как Накамото предполагает, что честное поведение не обязательно принимать вслепую, потому что оно поощряется. Более подробный анализ консенсуса Накамото с учетом роли стимулов не вполне вписывается в прошлые модели отказоустойчивых систем.

Практически все отказоустойчивые системы предполагают, что строгое большинство или сверхбольшинство (например, более половины или двух третей) узлов в системе являются и честными, и надежными. В открытой одноранговой сети нет регистрации узлов, и они свободно присоединяются и выходят. Таким образом, злоумышленник может создать достаточно Sybil или узлов sockpuppet , чтобы обойти гарантии консенсуса системы. Атака Sybil была формализована в 2002 году 14-летним Джоном Дусером, который обратился к криптографической конструкции, называемой доказательством работы (Proof of Work).

Чтобы понять доказательство работы, давайте обратимся к его истокам. Первое предложение, которое сегодня назвали бы доказательством работы, было создано в 1992 году Синтией Дворк и Мони Наор [23]. Их цель состояла в том, чтобы сдержать спам. Обратите внимание, что спам, атаки Sybil и отказ в обслуживании – все это примерно похожие проблемы, в которых злоумышленник усиливает свое влияние в сети по сравнению с обычными пользователями; доказательство работы применимо в качестве защиты от всех трех. В дизайне Дворка и Наора получатели электронной почты будут обрабатывать только те электронные письма, которые сопровождаются доказательством того, что отправитель выполнил умеренный объем вычислительной работы – отсюда и «доказательство работы». Вычисление доказательства заняло бы, возможно, несколько секунд на обычном компьютере. Таким образом, для обычных пользователей это не составит труда, но спамеру, желающему разослать миллион электронных писем, потребуется несколько недель при использовании эквивалентного оборудования. Кроме того, Дворк и Наор рассмотрели функции с лазейкой, секрет, известный центральному органу, который позволил бы ему решать головоломки, не выполняя работу.

Очень похожая идея, называемая hashcash, была независимо изобретена в 1997 году Адамом Бэком, исследователем с докторской степенью в то

время, который был частью сообщества шифропанков. Hashcash намного проще, чем идея Дворка и Наора: у него нет лазейки и центральной власти, и он использует только хеш-функции вместо цифровых подписей. Как следует из названия, в hashcash Бэк рассматривал доказательство работы как форму наличных денег. На своей веб-странице он позиционировал ее как альтернативу DigiCash Дэвида Чаума, которая представляла собой систему, которая выдавала неотслеживаемые цифровые деньги из банка пользователю [24]. Он даже пошел на компромисс с техническим дизайном, чтобы сделать его более похожим на деньги.

Между тем, в академической среде исследователи нашли множество приложений для доказательства работы помимо спама, таких как предотвращение атак типа «отказ в обслуживании» [25], обеспечение целостности веб-аналитики [26], и ограничение скорости подбора пароля в Интернете [27]. Термин «доказательство работы» был придуман только в 1999 году в статье Маркуса Якобссона и Ари Джуэлса, которая также включает хороший обзор работы до этого момента [28]. Стоит отметить, что эти исследователи, по-видимому, не знали о хэш-кэше, но независимо друг от друга начали сходиться к доказательству работы на основе хэша, которое было представлено в статьях Эрана Габбера и др. [29] и Джуэлсом и Брейнардом [25].

Более последовательные подходы к решению головоломок, как к наличным деньгам можно найти в двух эссе, предшествовавших биткойну, в которых описывались идеи, названные b-money [3] и bit gold [30] соответственно. Эти предложения описывают услуги временных меток, которые подписывают создание (через доказательство работы) денег, и как только деньги созданы, они подписывают переводы. Однако, если между серверами или узлами возникают разногласия по поводу реестра, нет четкого способа их разрешения. Позволить большинству решать, кажется, подразумевается в работах обоих авторов, но из-за проблемы Сивиллы эти механизмы не очень безопасны, если только нет привратника, который контролирует вход в сеть, или сопротивление Сибиллы само по себе достигается с доказательством работы.

Результаты и их обсуждение

Понимание всех предшествующих работ, содержащих элементы дизайна биткойна, позволяет оценить инновации Накамото по достоинству. В биткойне решения головоломок впервые не представляют собой деньги сами по себе. Вместо этого они просто используются для защиты бухгалтерской книги. Решающее доказательство работы выполняется специализированными организациями, называемыми майнерами (хотя Накамото недооценил, насколько специализированным станет майнинг).

Майнеры постоянно соревнуются друг с другом, чтобы найти следующее решение головоломки; каждый майнер решает немного отличающийся вариант головоломки, так что шанс на успех пропорционален доле глобальной мощности майнинга, которую контролирует майнер. Майнер, решивший головоломку, вносит следующую партию или блок транзакций в бухгалтерскую книгу, основанную на связанных временных метках. В обмен на услуги по ведению реестра майнер, который вносит блок, получает вознаграждение в виде вновь отчеканенных единиц валюты. С высокой вероятностью, если майнер вносит недопустимую транзакцию или блок, он будет отклонен большинством других майнеров, которые вносят следующие блоки, и это также аннулирует вознаграждение за «плохой» блок. Таким образом, благодаря денежным стимулам майнеры обеспечивают друг друга.

Выводы

Как было показано, большинство идей в биткойне, которые вызвали непонимание такие как распределенные реестры и византийские соглашения, на самом деле появились 20 или более лет назад. Таким образом для новой прорывной технологии требовались давно забытые решения, описанные в научных статьях. Белая книга биткойна, несмотря на родословную многих из ее идей, была более новой, чем большинство академических исследований. Более того, Накамото не заботился об академической экспертной оценке. В результате ученые в течение нескольких лет фактически игнорировали биткойн. Многие академические сообщества неофициально утверждали, что Биткойн не может работать, основываясь на теоретических моделях или опыте работы с прошлыми системами, несмотря на то, что на практике он работал. Идеи в исследовательской литературе могут постепенно забываться или оставаться недооцененными, особенно если они опережают свое время, даже в популярных областях исследований. Можно сказать, что биткойн был необычным и успешным не потому, что он был на переднем крае исследований любого из его компонентов, а потому, что он сочетал в себе старые идеи из многих ранее не связанных между собой областей.

REFERENCES

1 **Chaum, D., et al.** Untraceable electronic cash // Advances in Cryptology. – 1988. 319–327; [Electronic resource] https://dl.acm.org/citation.cfm?id=88969.

2 **Boyle, T. F.** GLT and GLR: Component architecture for general ledgers. –1997. [Electronic resource] https://linas.org/mirrors/www.gldialtone.com/2001.07.14/GLT-GLR.htm.

3 **Dai, W.** 1998; [Electronic resource] http://www.weidai.com/bmoney.txt.

4 **Grigg, I.** Triple entry accounting. – 2005. [Electronic resource] http://iang.org/papers/triple_entry.html.

5 **Bayer, D., Haber, S., Stornetta, W. S.** Improving the efficiency and reliability of digital time-stamping // Proceedings of Sequences. – 1991. [Electronic resource] https://link.springer.com/chapter/10.1007/978-1-4613-9323-8_24.

6 **Haber, S., Stornetta, W. S.** How to timestamp a digital document // Journal of Cryptology. – 1991. 3(2): 99–111; [Electronic resource] https://link.springer.com/chapter/10.1007/3-540-38424-3_32.

7 **Haber, S., Stornetta, W. S.** Secure names for bit-strings // In Proceedings of the 4th ACM Conference on Computer and Communications Security. –1997. 28-35; [Electronic resource] http://dl.acm.org/citation.cfm?id=266430.

8 **Nakamoto, S.** Bitcoin: a peer-to-peer electronic cash system. – 2008. [Electronic resource] https://bitcoin.org/bitcoin.pdf.

9 **Benaloh, J., de Mare, M.** Efficient broadcast timestamping. –1991. [Electronic resource] http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.38.9199.

10 **Merkle, R. C.** Protocols for public key cryptosystems. IEEE Symposium on Security and Privacy. – 1980. [Electronic resource] http://www.merkle.com/papers/Protocols.pdf.

11 **Laurie, B.** Certificate Transparency. acmqueue. – 2014. 12(8); [Electronic resource] https://queue.acm.org/detail.cfm?id=2668154.

12 **Melara, M., et al.** CONIKS: bringing key transparency to end users. Proceedings of the 24th Usenix Security Symposium. – 2015. [Electronic resource] https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-melara.pdf.

13 **Just, M.** Some timestamping protocol failures. – 1998. [Electronic resource] http://www.isoc.org/isoc/conferences/ndss/98/just.pdf.

14 **Lamport, L.** The part-time parliament. Digital Equipment Corporation. – 1989. [Electronic Resource] https://computerarchive.org/files/mirror/www.bitsavers.org/pdf/dec/tech_reports/SRC-RR-49.pdf.

15 **Lamport, L.** Paxos made simple. – 2001. [Electronic resource] http://lamport.azurewebsites.net/pubs/paxos-simple.pdf.

16 **Lamport, L., et al.** The Byzantine Generals Problem. ACM Transactions on Programming Languages and Systems. – 1982. 4(3). – 382-401; [Electronic resource] https://dl.acm.org/citation.cfm?id=357176 .

17 **Castro, M., Liskov, B.** Practical Byzantine fault tolerance. Proceedings of the Third Symposium on Operating Systems Design and Implementation. – 1999. [Electronic resource] http://pmg.csail.mit.edu/papers/osdi99.pdf.

18 **Nakamoto, S.** Re: Bitcoin P2P e-cash paper. – 2008. [Electronic resource] http://satoshi.nakamotoinstitute.org/emails/cryptography/11/.

19 **Wattenhofer, R.** The Science of the Blockchain. Inverted Forest Publishing. – 2016.

20 **Sirer, E. G.** Bitcoin guarantees strong, not eventual, consistency. Hacking, Distributed. – 2016. [Electronic resource] http://hackingdistributed.com/2016/03/01/bitcoin-guarantees-strong-not-eventual-consistency/.

21 **Garay, J. A., et al.** The bitcoin backbone protocol: analysis and applications // Advances in Cryptology. – 2015. – 281–310; [Electronic resource] https://eprint.iacr.org/2014/765.pdf.

22 **Pass, R., et al.** Analysis of the blockchain protocol in asynchronous networks. Annual International Conference on the Theory and Applications of Cryptographic Techniques. – 2017. [Electronic resource] https://link.springer.com/chapter/10.1007/978-3-319-56614-6_22.

23 **Dwork, C., Naor, M.** Pricing via processing or combatting junk mail. – 1992. [Electronic resource] https://dl.acm.org/citation.cfm?id=705669.

24 **Back, A.** Hash cash. – 2001. [Electronic resource] https://web.archive.org/web/20010614013848/http://cypherspace.org/hashcash/.

25 **Juels, A., Brainard, J.** Client puzzles: a cryptographic countermeasure against connection completion attacks. Proceedings of Networks and Distributed Security Systems. – 1999. – 151–165; [Electronic resource] https://www.isoc.org/isoc/conferences/ndss/99/proceedings/papers/juels.pdf.

26 **Franklin, M. K., Malkhi, D.** Auditable metering and lightweight security. – 1997. [Electronic resource] http://www.hashcash.org/papers/auditable-metering.pdf.

27 **Pinkas, B., Sander, T.** Securing passwords against dictionary attacks. Proceedings of the Ninth ACM Conference on Computer and Communications Security. – 2002. 161–170; [Electronic resource] https://dl.acm.org/citation.cfm?id=586133.

28 **Jakobsson, M., Juels, A.** Proofs of work and bread pudding protocols. –1999. [Electronic resource] http://www.hashcash.org/papers/bread-pudding.pdf.

29 **Gabber, E., et al.** Curbing Junk E-Mail via Secure Classiffication. – 1998. [Electronic resource] http://www.hashcash.org/papers/secure-classification.pdf.

30 **Szabo, N.** Bit gold. Unenumerated. – 2008. [Electronic resource] https://unenumerated.blogspot.com/2005/12/bit-gold.html.

Материал поступил в редакцию 05.12.22.

*О. Г. Потапенко[1], *А. О. Потапенко[2], А. О. Юсупова[3]*
[1,2,3]Торайғыров университеті,
Қазақстан Республикасы, Павлодар қ.
Материал 05.12.12. баспаға түсті

БЛОКЧЕЙН ТЕХНОЛОГИЯСЫНДАҒЫ ІРГЕЛІ ЗЕРТТЕУЛЕРДІ ТАЛДАУ

Көбінесе ақшаны немесе құнды кез келген нәрсені транзакциялау кезінде адамдар мен бизнес сенім мен сенімділік қамтамасыз ету үшін банктер мен үкімет сияқты делдалдарға қатты сенеді. Делдалдар транзакция кезінде сенімділікті арттыруға көмектесетін бірқатар маңызды тапсырмаларды орындайды, мысалы, аутентификация және жазбаларды жүргізу. Бүгінде ақшаны банктің көмегінсіз – банктік комиссияларды төлемей-ақ, күндер емес, секундтар ішінде тікелей біреуге жіберуге болады. Ақшаны банкке байланбаған онлайн-әмиянға сақтауға болады, яғни бұл әмиянды жасаған пайдаланушы ғана өз ақшасын толық бақылауға алады. Бұл блокчейн технологиясын пайдаланудың маңызды жағдайларының кейбірі ғана. Дегенмен, көпшілік үшін бұл әлі де бейтаныс, кейбіреулер оның болашақта қолданылатынына сенімді емес. Бұл технология төңірегіндегі скептицизм түсінікті, өйткені блокчейн әлі де дамудың және кең таралуының бастапқы кезеңінде. Мақалада блокчейн технологиясы салынған іргелі іргелі зерттеулерді қарастыруға тырысады.

Кілтті сөздер: блокчейн, биткоин, хэшинг, меркл ағаштары, жұмыс дәлелі.

*O. G. Potapenko[1], *A. O. Potapenko[2], A. O. Yusupova[3]*
[1,2,3]Toraigyrov University, Republic of Kazakhstan, Pavlodar
Material received on 05.12.12.

ANALYSIS OF FUNDAMENTAL RESEARCH IN BLOCKCHAIN TECHNOLOGY

More often than not, when transacting money or anything of value, people and businesses rely heavily on intermediaries such as banks and government to provide trust and certainty. Intermediaries perform a number of important tasks that help build trust during a transaction, such as authentication and record keeping.

Today it is possible to send money directly to someone without the help of a bank - in seconds, not days, without paying bank fees. It is possible to store money in an online wallet that is not tied to a bank, which means that only the user who created this wallet has full control over their money. These are just some of the important use cases for blockchain technology. However, for many it is still unfamiliar, some are not sure that it will be used in the future. The skepticism around this technology is understandable, because the blockchain is still at an early stage of development and widespread adoption. The article attempts to consider the fundamental fundamental research on the basis of which the blockchain technology was built.

Keywords: blockchain, bitcoin, hashing, merkle trees, proof of work.

Теруге 05.12.2022 ж. жіберілді. Басуға 15.12.2022 ж. қол қойылды.
Электрондық баспа
7,50 Mb RAM
Шартты баспа табағы 9,1. Таралымы 300 дана. Бағасы келісім бойынша.
Компьютерде беттеген А. Р. Омарова
Корректор: Д. А. Кожас
Тапсырыс № 4020

Сдано в набор 05.12.2022 г. Подписано в печать 15.12.2022 г.
Электронное издание
7,50 Mb RAM
Усл.печ.л. 8,4. Тираж 300 экз. Цена договорная.
Компьютерная верстка Е. Е. Калихан
Корректор: Д. А. Кожас
Заказ № 4020

«Toraighyrov University» баспасынан басылып шығарылған
«Торайғыров университеті» КЕ АҚ
140008, Павлодар қ., Ломов к., 64, 137 каб.

«Toraighyrov University» баспасы
«Торайғыров университеті» КЕ АҚ
140008, Павлодар қ., Ломов к., 64, 137 каб.
+7(718)267-36-69

e-mail: kereku@tou.edu.kz
www.vestnik.tou.edu.kz
https://vestnik-pm.tou.edu.kz/