

Иллюстрация технологии блокчейн и оценка влияния цифровых валют на финансовый менеджмент на примере Казахстана

Мигмер Баатрович Китинов

Институт востоковедения РАН, Москва, Россия

Аннотация. Центральные банки многих стран начинают проявлять интерес к цифровым валютам на основе технологии блокчейн. Финансовым менеджерам необходимо понимать ключевые особенности блокчейна, криптовалюты в целом и цифровых валют для корректного использования этих инструментов и управления рисками. К сожалению, на сегодняшний день не выполнена задача популяризации и разъяснения механизма блокчейна среди участников рынка. Опыт компьютеризации в конце XX века показал, что финансовые организации, отстающие от современных технологий, проигрывают в конкуренции и уходят с рынка. Цель данной работы – оценить последствия внедрения цифровых валют и показать механизм формирования цифровой валюты на примере Казахстана. В соответствии с целью поставлены следующие задачи: наглядно показать сущность технологии блокчейн, оценить влияние криптовалюты на финансовый менеджмент, продемонстрировать конкретный механизм формирования цифровой валюты на примере Казахстана.

Ключевые слова: блокчейн, биткоин, криптовалюты, цифровые валюты, тенге, цифровой тенге

Illustration of blockchain technology and assessment of digital currencies influence on financial management, Kazakhstan example

Midmer B. Kitinov

Institute of Oriental Studies RAS, Moscow, Russia

Abstract. Central banks of many countries are beginning to show interest in digital currencies based on blockchain technology. Financial managers need to understand the key

features of the blockchain, cryptocurrencies in general and digital currencies in order to correctly use these tools and manage risk. Unfortunately, to date, the task of popularizing and explaining the blockchain mechanism to market participants has not been completed. The experience of computerization at the end of the 20th century showed that financial institutions lagging behind modern technologies lose out in competition and leave the market. The purpose of this work is to assess the consequences of the introduction of digital currencies and show the mechanism for the formation of a digital currency using the example of Kazakhstan. In accordance with the goal, the following tasks were set: to demonstrate the essence of blockchain technology, to assess the impact of cryptocurrency on financial management, to demonstrate a specific mechanism for the formation of a digital currency using the example of Kazakhstan.

Keywords: blockchain, bitcoin, cryptocurrency, digital currency, tenge, digital tenge

Появление новых цифровых инструментов всегда приводит к появлению новых рисков. Насколько конкретная новая технология действительно полезна? Обычно ответ на этот вопрос можно дать только постфактум. В отношении криптовалюты дать ответ еще сложнее, поскольку значительная доля ее популярности связана с модой, популярностью у неквалифицированных участников финансовых рынков. Институциональные инвесторы, напротив, относятся к криптовалютам с осторожностью. Во многом это связано с отсутствием обеспечения. В отличие даже от фиатных денег, криптовалюты не поддерживаются никакими обещаниями государств [1]. В то же время ведутся активные работы в разных странах по выпуску официальных цифровых валют на базе технологии блокчейн, т. е. той же технологии, что применяется в криптовалютах.

Риск-менеджеры сталкиваются со сложностями в оценке криптовалют с помощью традиционных методов оценки товаров и валют – оценки ожидаемой доходности, волатильности и дохода от обладания (convenience yield) [2].

Технология блокчейн возникла как решение проблемы, вставшей перед создателем (или создателями – анонимность авторов первой криптовалюты до сих пор не нарушена) биткойна. Решение не является новым, однако именно в криптовалютах потребность в блокчейне стала революционной.

Суть проблемы заключалась в поиске способа защиты истории предыдущих операций от редактирования в условиях, когда список операций доступен для редактирования всем участникам системы расчетов. Иными словами, необходимо было передать каждому участнику системы список уже совершенных когда-либо и кем-либо операций с биткойном, обеспечить возможность дополнения истории операций вновь совершенными операциями (например, транзакцией по переводу средств от участника А к участнику Б) любым участником системы, но при этом сделать невозможным изменение данных об уже совершенных ранее операциях.

Решение включает в себя два шага.

На первом шаге все ранее совершенные операции (очень большой список) трансформируются в очень короткий набор символов (говоря технически корректным языком – хеш). Отметим, что это уникальная и однонаправленная

трансформация, т. е. технически получить один и тот же короткий набор символов из одинакового исходного перечня операций может каждый участник, но обратное преобразование из хеша в набор операций уже невозможно. Уникальность состоит в том, что изменение даже одного символа в исходной истории операций приведет с высокой вероятностью к получению другого хеша.

На втором шаге непосредственно к информации о вновь совершаемой операции прибавляется хеш всех ранее совершенных операций.

Таким образом, при добавлении в реестр каждая операция косвенно (в виде хеша) содержит информацию обо всех ранее заключённых. Любая попытка изменить историю операций сразу приведет к несовпадению в значениях хешей.

Приведем упрощенный пример.

Предположим, нам необходимо последовательно записать три блока информации: "мама", "мыла", "раму". Пусть хеш-функция состоит в том, что мы заменяем каждую букву ее порядковым номером, перемножаем полученные значения и берем первые две цифры полученного результата как хеш.

В этом блокчейне первый блок будет "мама".

Для получения второго блока вначале найдем хеш первого блока. Порядковый номер в алфавите буквы "А" – 1, буквы "М" – 14. Тогда вычисляем $1*14*1*14 = 196$. Первые две цифры – 19. Таким образом, второй блок в нашем упрощенном блокчейне будет выглядеть как "19 мыла".

Порядковый номер в алфавите буквы "Ы" – 29, буквы "Л" – 13. Хеш второго блока будет рассчитан как $1*9*14*29*13*1 = 47502$, первые две цифры дают 47. Итак, в нашем блокчейне первый блок будет "мама", второй блок "19 мыла", третий блок "47 раму".

В идеальном мире, когда все участники рынка честны и технические сбои не происходят, технология блокчейн не нужна. В реальном мире ситуация обстоит несколько иначе. Приведем два различных примера, в которых применение технологии блокчейн позволяет предотвратить мошенничество или определить технический сбой.

В первом, простом примере продемонстрируем устойчивость блокчейна к дублированию записей.

Пусть в системе расчетов есть только два блока информации – "мама" и "19 мыла". Все участники системы знают, что следующий блок должен начинаться с "47". Предположим, что третье сообщение звучит как "Алиса платит Бобу 20 биткоинов" (Алиса и Боб – стандартные имена в криптографии, используемые для иллюстрации примеров передачи сообщений). Тогда все участники расчетов системы с блокчейном примут это сообщение, если блок с ним выглядит как "47 Алиса платит Бобу 20 биткоинов". Если злоумышленник захочет скопировать и повторить сообщение, он сможет передать только полную копию "47 Алиса платит Бобу 20 биткоинов", но участники системы платежей уже ожидают в начале сообщения другой хеш, поэтому второе сообщение не будет обработано.

В данной работе не будет освещена детально техническая сторона вопроса шифрования, которая не дает злоумышленнику подменить хеш "47" на любой другой необходимый, а также то, как участники рынка узнают, что сообщение было действительно отправлено Алисой.

Второй пример, более сложный, демонстрирует устойчивость системы к двойным расходам, когда Алиса –мошенник, обладая всего 20 биткоинами, пытается одновременно сообщить разным участникам системы расчетов 2 сообщения: "47 Алиса платит Бобу 20 биткоинов" и "47 Алиса платит Чарли 20 биткоинов". Разные участки системы начинают обработку этих сообщений, после чего после них добавляются следующие блоки – четвертый, пятый и т. д. (напомним, что сообщение Алисы – это третий блок). Система блокчейн устроена так, что в момент, когда участник системы расчетов получает два противоречащих друг другу блокчейна, он автоматически выбирает наиболее длинный. Таким образом, из двух сообщений в итоге останется и будет считаться исполненным только одно (какое именно – будет определено во многом случайно).

Кстати говоря, в этом заключается и слабая сторона блокчейна в его конкретной реализации в биткоин – никогда нельзя быть уверенным в исполнении транзакции на 100 %, так как всегда есть риск, что транзакция попала в блокчейн с меньшим количеством блоков, после чего этот блокчейн будет отклонен и заменен на более длинный.

В данной работе также опустим технический момент, связанный с формированием блоков, который мешает Алисе заранее сформировать длинную цепочку блоков и выдать ее участникам рынка как приоритетную, но отметим, что это связано с процессом "майнинга", требующим большого количества вычислительных мощностей.

Появление цифровых валют центральных банков может значительно изменить финансовые рынки. Ключевое отличие цифровых валют центральных банков от "обычных" криптовалют состоит в том, что осуществлять их эмиссию может только центральный банк страны, а не широкий круг пользователей. В теории, выпуск цифровой валюты центральным банком в принципе убирает потребность в коммерческих банках, так как записи обо всех операциях с цифровой валютой хранит центральный банк. На практике центральные банки не хотят вызывать значительные потрясения на финансовых рынках и поэтому оставляют розничным банкам право производить присущие им операции даже в условиях выпуска цифровой валюты. Тем не менее, выпуск цифровой валюты повышает уровень конкуренции и снижает доходность розничных банков, так как переток денежных средств из наличного и безналичного видов, с которыми есть право работать у коммерческих банков, в цифровой вид, с которым может работать только Центральный банк и конечные пользователи, вызывает риски сокращения базы ликвидности для коммерческих банков (если цифровые валюты получат широкое распространение). В результате коммерческие банки будут вынуждены повышать ставки по депозитам, что приведет к росту конкуренции и потенциальному сокращению прибыльности. Несмотря на все риски для коммерческих банков, центральные банки продолжают изучать тему внедрения цифровых валют.

Финансовым менеджерам необходимо понимать вызовы, связанные с внедрением цифровых валют. Кристиан Де Ритис, эксперт по финансам, приводит следующую матрицу SWOT для цифровых валют центральных банков [3].

К сильным сторонам относятся: прозрачность, удобство, низкая стоимость транзакций, возможность отследить историю транзакций, повышение гибкости монетарной политики, усложнение кражи средств.

К возможностям относятся: увеличение количества пользователей, быстрая аналитика, рост безопасности при утечке данных.

К слабым сторонам относятся: потенциальное снижение конфиденциальности, медленная скорость транзакций, недоступность средств при потере пароля, потребность в технологическом обеспечении и связи, новизна (решения еще не были протестированы на устойчивость).

К угрозам относятся: вытеснение центральным банком коммерческих банков, повышение контроля государства над финансовой системой (впрочем, этот пункт в зависимости от позиции читателя может быть отнесен и к сильным сторонам, и к возможностям, и к слабым сторонам), повышение чувствительности коммерческих банков к массовому оттоку ликвидности.

С 2021 года в Казахстане Центральным банком (Национальный банк Казахстана) проводится работа по проекту формирования цифрового тенге. Целью проведения работы стало изучение потенциала цифровых валют в инновации в индустрии платежей и повышения конкурентоспособности Казахстана на мировом финансовом рынке.

Для конечных потребителей большой разницы непосредственно в расчетах по сравнению с текущими формами оплаты не будет – расчеты в цифровом тенге будут доступны через уже существующие платежные инструменты [4].

Согласно позиции Национального банка, цифровой тенге будет служить дополнением существующих в Казахстане платежных систем и платежным средством наряду с наличным и безналичным тенге (в целом, ЦБ РФ придерживается аналогичной позиции в отношении цифрового рубля). В отличие от типичных безналичных операций, платежи в цифровом тенге будут осуществляться моментально (как правило, конечные пользователи редко знают о том, что окончательные расчеты по безналичным платежам происходят с задержкой, но это так, и у цифрового тенге такая задержка отсутствует).

В Казахстане планируется к реализации подход, при котором кошельки в цифровом тенге открывают непосредственно частные банковские организации, при этом в разных банках клиенту открываются разные кошельки. Ключи от денежных средств хранятся непосредственно на устройстве клиента, информация о средствах также хранится на устройстве в завершенном от банка виде. При осуществлении транзакции в офлайн-режиме информация о передаваемых средствах также передается вместе с банковской подписью. Корректность подписи может быть проверена любым участником. Таким образом, выбранная в Казахстане модель позволяет осуществлять расчеты в цифровом тенге, в том числе в офлайн-режиме.

Техническая проблема мошенничества, когда один и тот же цифровой тенге в офлайн-режиме может быть потрачен несколько раз, а информация об этом у Национального банка появится только после выхода устройств в сеть, пока не решена. Банк рассчитывает, что эта проблема будет решаться на

"последней миле", т. е. на уровне банковских приложений и платежных устройств (мобильных телефонов) клиентов [5].

В ходе проекта Национальным банком была сформирована площадка Digital Tenge Hub для тестирования цифрового тенге участниками рынка. Для подготовки к проведению пилотного проекта были приглашены внешние эксперты, которые проводили обучение его участников [6].

Национальный банк Казахстана принял решение об отсутствии необходимости в прибыли от эмиссии и обслуживания цифрового тенге, бизнес-модель должна покрывать только расходы на содержание. В части модели учета выбрана система, при которой денежный актив используется только один раз. В момент, когда это происходит, цифровой тенге уничтожается, и создаются две новые записи: одна у израсходовавшей средства стороны, а вторая – у стороны, к которой средства поступили.

В конце 2022 года стало известно, что технологической основой для цифрового тенге станет платформа системы Vinance. Вместе с тем, Vinance в начале октября 2022 года сообщила о получении лицензии от Комитета МФЦА по регулированию финансовых услуг (AFSA) на управление платформой цифровых активов и оказание кастодиальных услуг в Международном финансовом центре "Астана" (МФЦА) [7].

Таким образом, выбранная в Казахстане операционная модель цифрового тенге опирается на существующую двухуровневую архитектуру. В этом варианте Национальный банк производит эмиссию цифрового тенге, а частные финансовые организации открывают кошельки и распределяют цифровую валюту в соответствии с поручениями клиентов. С точки зрения инфраструктуры платформа цифрового тенге объединит технологию распределенных реестров (блокчейн) и традиционные подходы. Реальное воздействие цифровых валют на финансовую систему еще никем не измерялось в силу отсутствия достаточного опыта в эксплуатации цифровых валют. Тем не менее, эксперты подчеркивают усиление роли государства и риск повышения конкуренции между частными банками. Технология блокчейн, на которой основаны цифровые валюты, в оригинале была популяризована в криптовалюты блокчейн. Ключевое преимущество технологии – высокая устойчивость к мошенническим действиям со стороны пользователей системы и операционным ошибкам.

Список источников

1. Bank for International Settlements. Cryptocurrencies: looking beyond the hype; 2018. <https://www.bis.org/publ/arpdf/ar2018e5.pdf> (дата обращения: 30.04.2023).

2. John C. H. Options, Futures, and Other Derivatives. [Опционы, фьючерсы и прочие производные инструменты]. Toronto, Canada: Pearson, 2014. 896 p.

3. Cristian de Ritis. Modelling currencies: Risks and opportunities; 2021. <https://www.garp.org/risk-intelligence/technology/digital-currencies-risks-and-opportunities> (accessed 30.04.2023).

4. Кучма В. Всё о цифровом тенге в Казахстане: разбираемся, как это будет; 2022. https://forbes.kz/process/expertise/vse_o_tsifrovom_tenge_v_kazahstane_kak_eto_budet/ (дата обращения: 30.04.2023).
5. Национальный банк Казахстана. Результаты исследования о необходимости внедрения цифрового тенге; 2022. <https://nationalbank.kz/file/download/85868>(дата обращения: 30.04.2023).
6. Kapital.KZ. Опубликован доклад по пилотному проекту "Цифровой тенге"; 2022. <https://kapital.kz/tehnology/111347/opublikovan-doklad-po-pilotnomu-proyektu-tsifrovoy-tenge.html> (дата обращения: 30.04.2023).
7. T-Adviser. Цифровой тенге. https://www.tadviser.ru/index.php/Статья:Цифровой_тенге (дата обращения: 30.04.2023).

References

1. Bank for International Settlements. Cryptocurrencies: looking beyond the hype; 2018. <https://www.bis.org/publ/arpdf/ar2018e5.pdf>(accessed: 30.04.2023).
2. John C. Н. Options, Futures, and Other Derivatives. Toronto, Canada: Pearson, 2014. 896 p.
3. Cristian de Ritis. Modelling currencies: Risks and opportunities; 2021. <https://www.garp.org/risk-intelligence/technology/digital-currencies-risks-and-opportunities> (accessed 30.04.2023).
4. Kuchma V. Everything about digital tenge in Kazakhstan: sorting out what would it be; 2022. https://forbes.kz/process/expertise/vse_o_tsifrovom_tenge_v_kazahstane_kak_eto_budet/(accessed: 30.04.2023). (In Russ.).
5. Kazakhstan National Bank. PResults of study on necessity of digital tenge; 2022. <https://nationalbank.kz/file/download/85868>(accessed: 30.04.2023). (In Russ.).
6. Kapital.KZ. Report published on "Digital tenge"project; 2022.<https://kapital.kz/tehnology/111347/opublikovan-doklad-po-pilotnomu-proyektu-tsifrovoy-tenge.html>(accessed: 30.04.2023). (In Russ.).
7. T-Adviser. Digital tenge.https://www.tadviser.ru/index.php/Статья:Цифровой_тенге (accessed: 30.04.2023). (In Russ.).

Статья поступила в редакцию 13.05.2023; одобрена после рецензирования 14.05.2023; принята к публикации 17.05.2023.

The article was submitted 13.05.2023; approved after reviewing 14.05.2023; accepted for publication 17.05.2023.