

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»
Факультет бизнеса и менеджмента

**ВНЕДРЕНИЕ ТЕХНОЛОГИИ БЛОКЧЕЙН В МОБИЛЬНЫЙ
БАНКИНГ**

Научно-исследовательская работа студента
Саргсяна Левона Арамовича

3 курса, направление подготовки:
38.03.05 Бизнес-информатика
образовательной программы
«Бизнес-информатика»

Оглавление

Введение

Актуальность темы исследования	3
Объект	4
Предмет	4
Методы	4
Цели	5
Задачи	5
Гипотеза	5
Теоретическая составляющая индустрии криптовалюты.	6
Рынок проектов на основе технологии блокчейн и их историческое развитие. 6	
Фаза 1.0: Появления биткоинов и альткоинов. Транзакции. (2008-2013)	8
Фаза 2.0: Появление Ethereum. Смарт-контракты. (2013-2015)	9
Фаза 3.0: Приложения. (2016-2019)	10
Криптовалюта, как децентрализованная денежная единица.	11
Разбор технической составляющей криптовалюты.....	14
Технологическая модель работы криптокошельков.	18
Описание криптокошелька и основная теория его функционала.	18
Техническая архитектура криптокошелька.....	22
Бизнес-уровень.....	25
Уровень приложений.....	25
Технический уровень	26
Интеграция технологии криптокошелька в классическую банковскую систему.28	
Техническая архитектура банковской индустрии.	28
Варианты внедрения сервисов криптокошелька в банковскую систему.	30
Дополнение к готовому продукту	31
Создание нового криптокошелька	32
Использование API	34
Заключение.....	36
Используемая литература	36

Введение

Актуальность темы исследования

Технология блокчейн, относительно других популярных инноваций, имеющих масштабный характер, появилась недавно. Однако она довольно быстро обрела популярность не только как новая система, а также как возможность повлиять на многие существующие проблемы в разных сферах жизнедеятельности человека, путем создания новых продуктов на ее основе. На данный момент мнения насчёт данной технологии расходятся. Некоторые крупные инвесторы не рискуют в неё вкладываться, однако другие компании стараются на её основе предложить рынку более совершенные продукты. Указанная тема актуальна, так как продукты продолжают создаваться и привлекать инвестиции, и нельзя дать точного ответа на вопрос, будут ли долгое время жизнеспособны данные продукты. Учитывая, что они направлены на разные сферы, в которых уже существуют решения, в том или ином виде, не решена задача интеграции данной технологии в уже готовые бизнес-модели. Основная необходимость изучения данного вопроса заключается в понимании возможности реализации данной интеграции с точки зрения оптимального выигрыша компании, регулирующей рассматриваемый продукт. Поставленный вопрос в данное время часто приписывают к цифровой трансформации бизнеса. Необходимо алгоритмизировать процесс и уточнить, является ли в банковской отрасли это пивотом, или же внедрением новых продуктовых решений в бизнес-процесс? В банковской отрасли на рынке России по состоянию 2019 года наблюдается продолжительный рост использования онлайн-банкинга и безналичной оплаты.¹ Дополнительно наблюдается сильный толчок в отрасли блокчейн-продуктов, а в частности такого продукта, как криптокошелёк, который я собираюсь рассматривать в данном исследовании. Увеличение популярности оплаты как классической валютой, так и криптовалютой позволяет поднять вопрос о реализации их интеграции в один общий продукт. Моё исследование предназначено для ответа на этот вопрос. Глобальное исследование криптовалют, проведенное кембриджским университетом в 2017 году, и обновленное годом позже, показывает, что

¹ Mastercard: жители России стали чаще оплачивать покупки безналично [Электронный ресурс] / Mastercard – свободные аналитические данные. – URL: <https://newsroom.mastercard.com/ru/press-releases/mastercard-%D0%B6%D0%B8%D1%82%D0%B5%D0%BB%D0%B8-%D1%80%D0%BE%D1%81%D1%81%D0%B8%D0%B8-%D1%81%D1%82%D0%B0%D0%BB%D0%B8-%D1%87%D0%B0%D1%89%D0%B5-%D0%BE%D0%BF%D0%BB%D0%B0%D1%87%D0%B8%D0%B2%D0%B0%D1%82/>

число активных, уникальных владельцев кошельков постоянно растёт. В 2013 году количество пользователей составляло примерно 3 миллиона человек. К 2017 данное число увеличилось почти в 2 раза, составив 5,8 миллионов. Количество активных кошельков составляет 11,5 миллионов шифров.²

Объект

Объектом исследования является процесс интеграции двух разных технологий в единый банковский продукт. С одной стороны рассматривается технология блокчейн и определённый продукт, такой как криптовалюта. Объектом, в который будет интегрирована данная технология, является классический банковский продукт: онлайн кошелек. Проблемной ситуацией объекта исследования выступает вопрос выбора направления интеграции.

Предмет

Предметом исследования является бизнес-модель рассматриваемых продуктов и компаний. В данном случае необходимо рассмотреть объект с точки зрения эффективного применения технологии блокчейн в банковской сфере. Так как бизнес-модель в себя включает большое количество дополнительных частей, которые необходимо рассмотреть, о которых написано позже, не будем их конкретизировать как отдельные предметы исследования, и будем рассматривать как общую составляющую.

Методы

В данном исследовании я буду в основном пользоваться теоретическим методом решения поставленных задач. Он будет включать в себя следующие отдельные направления работы

- Анализ и обобщение истории развития технологии. Поиск основной необходимой теории среди доступных онлайн-публикаций на популярных ресурсах, связанных с темой исследования, а также написанных книг.
- Поиск и сравнение технической составляющей готовых продуктов на открытом онлайн-ресурсе GitHub. Исследуются основные языки программирования и основные файлы, позволяющие связывать между собой алгоритмы работы продукта.

² Dr Garrick Hileman, Michel Rauchs. GLOBAL CRYPTOCURRENCY BENCHMARKING STUDY // Cambridge Centre for Alternative Finance. – М., 2017

- Поиск и исследование рассматриваемых объектов и их представление, используя язык моделирования ArchiMate. Он позволяет охватить разные слои архитектуры, с точки зрения предприятия.

Цели

Цель данного исследования выявить разные направления интеграции с технической точки зрения функционала и внутренней составляющей криптокошелька, учитывая большой выбор криптовалют, в классический банковский кошелек.

Задачи

- Определить техническую-модель криптовалюты и криптокошелька, а также их основной формат работы
- Определить техническую-модель банковского продукта “онлайн кошелек” и составить его архитектуру
- Выявить основные технические критерии криптокошелька, влияющие на интеграцию.
- Найти разные варианты внедрения нового продукта в архитектуру банковского предприятия и составить модели результатов интеграций

Гипотеза

Существует несколько вариантов интеграции криптовалюты в классический банковский сервис. Дополнительная интеграция криптовалюты, и реализация возможности ее использования в классическом банковском кошельке позволит банкам, охватывать больше сфер, и предлагать большее количество сервисов для своих потребителей. Данная интеграция приведет к большой дополнительной прибыли. В данном исследовании рассматривается вопрос технической проблемы и необходимости изменения бизнес-моделей банков, желающих интегрировать криптовалюту в свою продуктовую линейку.

Теоретическая составляющая индустрии криптовалюты.

В данной главе я рассматриваю криптовалюту с технической стороны. В первую очередь необходимо обратить внимание на историю развития технологии блокчейн, на которой работают рассматриваемые продукты. Какие основные изменения были следствием нынешней популярности, и причины их возникновения.

Рынок проектов на основе технологии блокчейн и их историческое развитие.

Мир увидел технологию и первый проект на базе блокчейна, именуемый биткоином, осенью 2008 года (первый выход в общедоступность 9 января 2009). Сатоши Накамото - никнейм создателя данной технологии разослал определенному кругу лиц письмо, в котором описал алгоритм работы его идеи.³ Это был первый значимый прорыв в истории, который в дальнейшем очень сильно изменит рынок IT проектов и навсегда оставит след, как одна из самых сильно разделенных во взглядах общественности технологий. Как многим кажется, мотивацией создателя являлось желание избавиться от третьего лица как посредника в финансовых вопросах двух торгующих лиц. Другими словами, особенностью биткоина, криптовалюты написанной на базе блокчейна, являлась возможность передачи цифровой валюты без дополнительного контролирующего органа в лице банка или другого финансового учреждения.

Для продолжения, давайте определимся с основным механизмом работы и терминами данной технологии:

Блокчейн – это технология надежного распределенного хранения записей обо всех когда-либо совершенных биткойн-транзакциях. Блокчейн представляет собой цепочку блоков данных, объем которой постоянно растет по мере добавления майнерами новых блоков с записями самых последних транзакций. Основное новшество данной технологии заключается в архитектуре, которое обеспечивает децентрализованные (разделенное по всем участникам процесса) транзакции.

³ <https://bitcoin.org/bitcoin.pdf>

Криптовалюта – это цифровая наличность. Это одновременно цифровая валюта и онлайн-платежная система, в которой технологии шифрования обеспечивают управление генерацией денежных единиц и подтверждение перевода средств, и которая работает независимо от государственных, регулирующих финансовую отрасль, структур. По сути, можно сказать, что криптовалюта это платёжное средство, которое при этом не обладает полным набором функций денег, а выступает больше в роли цифрового товара, стоимость которого зависит от общепринятых среди пользователей стандартов.

Криптокошелек – это сервис, который предоставляет возможность хранения и проведения определенных операций с криптовалютой. В ее основе лежит технология шифрования информации при помощи идентификационного ключа, уникального для каждого пользователя. Кошельки для хранения криптовалюты бывают 4-х типов, каждый из которых я более подробно рассмотрю в дальнейшем: бумажный кошелек (paper-wallet); программный кошелек (soft-wallet); аппаратный кошелек (hard-wallet); биржа (exchanges).

Изначально во время появления блокчейна и биткоина не была разработана модель регулирования данной технологии и её общественного использования. Причины довольно понятны, технология разрабатывалась для людей, и планировалась быть синонимом слову “свобода”. Однако на деле, спустя почти 10 лет её мирового использования стало понятно, что без исследований в вопросах ее использования в бизнес-среде не обойтись. После данного предложения встает довольно очевидный вопрос: “А что произошло за эти 10 лет?”. История блокчейн-проектов довольно обширна, чтобы затронуть все ее сферы, поэтому я попробую рассказать о самых важных, связанных именно со стороной криптовалюты. Данная ретроспектива направлена на понимание алгоритмов развития. Вспомнив, в какую сторону двигался прогресс и разобравшись в её причинах можно найти больше аргументов для ответа на вопрос, в какую сторону вероятнее всего он будет двигаться дальше.

По негласной философии технологии, все проекты на ее основе имеют открытый исходный код в системах контроля версий. В основном GitHub⁴ является гравитационной платформой, притягивающей всех разработчиков. Особенность GitHub позволяет определить создателей технологии, стек-технологий, используемых при создании проекта, а также предоставляет

⁴ <https://github.com/>

ценность для потенциальных инвесторов в виде понимания факторов риска. Со времён написания первого кода, на котором был построен биткойн, количество проектов на GitHub увеличивалось в среднем на 8600 в год. В 2016 году, эта цифра приблизилась к 27000.⁵

Рост проектного содержимого не отставало от ускоренного роста количества проектов. “При анализе блокчейновых репозиторий и их содержимого мы заметили, что число участвующих организаций быстро растёт. В 2010 г. организациями было разработано меньше 1% от всех проектов. В 2017 г. на их блокчейновые проекты приходится 11% (в настоящее время на организации приходится 7% от всех – не только блокчейновых – разработок ПО на GitHub). И последние данные по успешности блокчейновых инициатив коммерческих организаций с открытым кодом выглядят многообещающе; в их числе есть некоторые крупные известные коммерческие субъекты.” - пишет Deloitte в своём исследовании данных GN Torrent и GitHub API. Мы можем замечать, что развитие проектов данной технологии происходит так называемыми скачками. Этот вывод можно сделать на основе тенденции к сильному росту количества проектов и популярности технологии в рассматриваемый короткий промежуток времени. Чаще всего культурные явления, которые характеризуются скачками можно разделить на логически взаимосвязанные периоды. Какие же периоды в рынке блокчейн-проектов можно выделить?

Фаза 1.0: Появления биткоинов и альткоинов. Транзакции. (2008-2013)

После первой добытой криптовалюты началось становление биткоина в понимании общественности. Сложность технологии и малое сообщество, которое было проанализировано выше, объясняет причины малой популярности блокчейна. Изначально пути её развития не были столь многогранны как сейчас. Использование блокчейна лишь в качестве основы для электронной валюты было аксиомой, которая не как шаблон держалась долгое время. Однако хоть и проектов было мало, они начинали своё становление. Первыми стали появляться криптокошельки, в основном с холодным ключом хранения, а также сервис для купли-продажи биткоинов (биржа) Bitcoin Market. И соответственно, поняв, что рынок криптовалюты не должен ограничиться лишь выбором в одну монету, на свет появились такие криптовалюты, как Litecoin и SwiftCoin. А также переосмыслив технологию

⁵ Evolution of blockchain technology [Электронный ресурс] / Deloitte – свободные аналитические данные. – URL: <https://www2.deloitte.com/insights/us/en/industry/financial-services/evolution-of-blockchain-github-platform.html> (Дата обращения: 17.05.2019)

блокчейн и избавившись от необходимости в майнинге⁶ в 2012 году появился Ripple, представляющий концепцию консенсуса среди членов сети. В это время успели уже появиться первые онлайн-магазины, принимающие биткоин через анонимные аккаунты, и стала набирать популярность, более крупная биржа, обменивающая фиатные деньги на биткойн - MtGox, когда стоимость одного Биткойна стала равняться примерно 1-му доллару.

Фаза 2.0: Появление Ethereum. Смарт-контракты. (2013-2015)

Начало этой фазы оставила большой след в истории блокчейн-культуры. Во-первых, увеличилось количество инвестиций в биткойн проекты, преимущественно в криптовалютные биржи Coinbase, Circle и Bitstamp. Во-вторых, появления нового видения мира криптовалют и как следствие, создание Ethereum молодым программистом, Виталиком Бутерином.

Ethereum - это блокчейн с открытым исходным кодом. Он поддерживает модифицированную и улучшенную версию консенсуса Накамото. Ethereum предоставляет платформу для создания децентрализованных приложений. Бутерин отличил Ethereum от Биткойн-блокчейна, включив функцию, которая позволяет людям записывать другие активы, такие как лозунги, а также контракты. Новая функция расширила функциональность Ethereum с криптовалюты до платформы для разработки децентрализованных приложений.

С появлением новой блокчейн технологии начали появляться языки программирования, такие как Solidity, Serpnet и др. Они поддерживают алгоритмы для написания смарт-контрактов. Это позволило ускорить рост появления новых проектов, дав возможность разработчикам собственноручно и с большей скоростью создавать сети в рамках блокчейна.

К этому времени на рынке криптовалюты появляется более сильный альткойн - XRP, разработанный компанией Ripple. Сотрудничество с крупными банками позволило этой криптовалюте расположиться на второй строчке в биржевом индексе криптовалют, неоспоримо уступая лишь Биткойну.

⁶Майнинг биткойна и других монет, построенных на алгоритме PoW – Proof-of-Work (с англ. – доказательства работы), – это постоянный перебор данных по определенному алгоритму, вычислительная работа, производимая компьютерным оборудованием. И чем мощнее и экономичнее вычислительное устройство, тем больше шансов на успех.

В 2014 году была сформирована технология Blockchain R3. Форс Консорциум также создан с более чем 40 устаревшими финансовыми компаниями для реализации технологии блокчейн. Платформа R3 blockchain под названием Corda имеет сильное присутствие в финансовом секторе, что сигнализирует об успехе проекта.

В 2015 году происходит два важных события:

Первое - американское финансовое агентство FinCEN оштрафовало Ripple Labs на 700 000 долларов США за продажу криптовалюты XRP без предварительной регистрации у них. Эта информация нам пригодится для дальнейшего ознакомления с совместной работой государственных банков и криптовалют.

Второе - крупнейшая в мире некоммерческая организация с открытым исходным кодом, Linux Foundation, запускает Hyperledger; набор инструментов, чтобы помочь людям создавать проекты блокчейна. Это же в свою очередь нам показывает, что мир полностью готов к передаче знаний о разработке блокчейн проектов. В дальнейшем такие шаги перерастут в более глобальные университетские подходы к изучению блокчейна.

Фаза 3.0: Приложения. (2016-2019)

Одним из самых известных проектов, работающих над блокчейном третьего поколения, является Cardano. Компания фокусируется на решении 4 основных проблем, с которыми сегодня сталкиваются блокчейны мира:⁷

1. Масштабируемость
2. Совместимость
3. Устойчивость
4. Управление

Есть много других компаний, пытающихся решить проблему с первыми двумя поколениями блокчейна.

Среди ведущих компаний, помимо Cardano, Stellar, Zilliqa и EOS, однако можно найти еще больше, так как конкуренция действительно жесткая.

Cardano претендует на звание 3-го поколения блокчейна, решая проблемы с масштабируемостью и совместимостью.

⁷ A Very Brief History Of Blockchain Technology | Blockchain History 2019 [Электронный ресурс] / Medium – свободный интегратор публикаций. – URL: <https://medium.com/@muhammadnoor/a-very-brief-history-of-blockchain-technology-blockchain-history-2019-3c9f9857e085>

2018 год был годом ICO, и теперь мы вступаем в год принятия блокчейна. Интернет-гигант, такой как AliBaba, Amazon, Google, Facebook и т.д., уже начали работать над проектами с технологией блокчейна. Недавно Facebook объявил о запуске собственной криптовалюты.

Криптовалюта EOS привлекает 4 миллиарда долларов в самой большой ICO за всю историю. Многие полагают, что в будущем он заменит Ethereum из-за передовых технологий и высокой скорости транзакций.

По данным Forbes, крупнейшая в мире ежегодная конференция по блокчейну в 2018 году посещает 4000 человек. Почти 15% финансовых компаний сегодня используют блокчейн .

Криптовалюта, как децентрализованная денежная единица.

В прошлом пункте упоминалась терминология криптовалюты. В этом параграфе я рассмотрю данную цифровую валюту более подробно для понимания модели ее работы.

Как уже упоминалось ранее, криптовалюта - набор кода, базирующийся на определённой блокчейн технологии. К примеру Биткоин, как валюта, регистрируется в журнале записей биткойн-блокчейна. Блокчейн как цепочка блоков транзакций – это распределенный, общедоступный и совместно используемый всеми узлами сети реестр или журнал записей, содержащий данные о транзакциях. Журнал обновляется майнерами и отслеживается всеми желающими, но при этом никем не контролируется. Он подобен гигантской общедоступной таблице, которая периодически обновляется и подтверждает уникальность цифровых операций перевода денежных средств.⁸ Этот алгоритм показывает первый, нижний уровень стека технологий, необходимых для полного функционирования криптовалюты. Всего уровней стека блокчейн технологий три.

Средним уровнем стека является протокол – пакет программ, который переводит средства путем внесения транзакций в блокчейн (журнал записей). Третий уровень – это непосредственно схема самой валюты.

⁸ Мелани Свон, Блокчейн. Схема новой экономики. – М.: Издательство Олимп-Бизнес, 2017. 1-я глава. Блокчейн: фундамент для криптовалют

Важно понимать, что общая структура любой современной криптовалютной системы формируется всеми тремя уровнями (блокчейн, протокол и валюта). Каждая монета представляет собой одновременно валюту и протокол, она может иметь собственный распределенный журнал записей или использовать распределенный блокчейн биткойна. Ещё один пример: криптовалюта Litecoin использует Litecoin-протокол, работающий с блокчейном Litecoin, – по сути, это клон биткойна, в котором слегка изменены некоторые функции. Отдельный блокчейн означает, что у монеты имеется собственный децентрализованный журнал записей с такой же структурой и форматом, что и распределенный журнал записей биткойна. Другие протоколы, например Counterparty, имеют собственную валюту (XCP), но используют блокчейн биткойна, то есть транзакции XCP регистрируются в распределенном журнале записей биткойна.

Основной парадигмой множества нынешних компаний, владеющих информацией, таких как Facebook, Google или любые банки - централизация. Все данные пользователей хранятся на их серверах. В связи с тенденцией увеличения стоимости информации, параллельно с ней увеличивается риск использования таких продуктов. Блокчейн и механизм работы криптовалюты решают данную проблему децентрализованностью.

Однако в модели децентрализации есть вполне очевидный вопрос: если отсутствует регулирующий орган, как избежать проблем, связанных со схожестью в информационном потоке данных? К примеру, двух адресов в системе, заканчивающихся одинаково. Ответить на этот вопрос поможет теория криптографии. У блокчейн технологии существует два ключа, закрытый и публичный. Они являются основными регуляторами как отношений со стороны пользователей, так и с технологической точки зрения. Закрытый ключ представляет собой приватный пароль для проведения операций с криптовалютой. Он уникален для каждого пользователя и предоставляется программой. На её основе исходя из алгоритмов, прописанных в коде блокчейн-технологии, генерируется публичный адрес. Он же в свою очередь необходим, чтобы с его владельцем можно было взаимодействовать. Что происходит в момент отправки “денег” (здесь и в дальнейшем слово деньги может быть использовано как описание цифровой валюты/криптовалюты)? При совершении платежа, используется закрытый ключ для “подписания” транзакции. В дальнейшем данная транзакция автоматически отправляется на другие аккаунты в цепочке

блокчейн, что позволяет поддерживать полную прозрачность в системе. Для того, чтобы этот процесс проходил согласно правилам, был разработан алгоритм консенсуса⁹. Им пользуются легальные криптовалюты. Основные три алгоритма:

1. Доказательство значимости (Proof of Importance)
2. Доказательство выполнения работы (Proof-of-work)
3. Доказательство доли владельца (Proof of Stake)

Причины появления криптовалюты разнятся, и в связи с этим появились разного рода токены, которые, соответственно, разнятся в вопросах экономики.

1. Currencies Coin - самый популярный вид криптовалют. Именно они позволяют производить операции по купле-продаже на многих сервисах, не причастных к блокчейн инфраструктуре.
2. Platforms Coins - токены, привязанные к платформе, позволяющие разрабатывать криптовалюту. Я рассмотрю их подробнее в следующем параграфе. Самой популярной такой валютой является Ethereum.
3. Cryptocurrency Exchanges - внутрибиржевые токены. Они создаются для помощи новым монетами получить стартовые инвестиции от пользователей биржи, при этом не подвергая их большому риску. Данные “монеты” также являются ликвидными вне привязанной биржи.
4. Utility Tokens - по сути это некие аналоги акций. Данные токены ограничены по эмиссии и связаны с полезностью приложения, к которому привязаны. После проведения ICO токены продолжают играть роль некоего инвестиционного продукта, что делает их по модели схожими на акции.
5. Security Tokens - токены безопасности, которые имеют некую стоимость, в зависимости от общего рынка. Они выпускаются во время проведения ICO и предназначены для инвесторов. На основе данных токенов инвесторы в дальнейшем делят прибыль, получают дивиденды и т.д.
6. Crypto Commodities - термин используется для описания торгуемого или взаимозаменяемого актива, приуроченного к определенному продукту. Сервис или приложение, предлагаемое услуги, может создать и интегрировать токены в свой продукт, которые могут являться

⁹ Консенсус - соглашение, позволяющее определить истинность процессов.

внутренней валютой. Такие токены не задействованы на рынках или биржах.

7. Stable Coins - “Стабильные токены” представляют собой криптовалюты, волатильность которых сведена к минимуму благодаря привязке к тому или иному стабильному активу, например, доллару или золоту.

Разбор технической составляющей криптовалюты.

Основная цель моего исследования заключается в анализе вариантов интеграции криптовалюты в качестве новой валюты в классическую банковскую систему. И так как я рассматриваю технологическую сторону интеграции, вопрос механизма работы криптовалюты важен.

На данный момент спустя несколько лет развития индустрии процесс создания новой криптовалюты и дальнейшая её поддержка сильно упростилась. Есть три основных уровня стека блокчейн-технологии, которые я уже упоминал в прошлом параграфе:

1. Основная блокчейн платформа - самый высокий уровень, на основе которого базируются алгоритмы криптовалюты.
2. Криптовалютный протокол и клиент - второй уровень, который определяет все процессы и операции, которые возможны на базе блокчейн-платформы.
3. Криптовалюты - непосредственно сама оболочка.

По сути, большинство криптовалют можно объединить в единое “генеалогическое древо” и проследить, что у многих криптовалют существует основной единый “предок”, которым является биткойн-блокчейн. Процесс создания новой криптовалюты на основе уже существующего блокчейна называется в индустрии форком¹⁰.

Однако говоря о простоте создания новой криптовалюты нельзя не упомянуть специализированные блокчейн-платформы, позволяющие создавать токены. Одна из самых популярных таких платформ, которую я уже упоминал выше - Ethereum. Второе место занимает платформа Waves. Также есть такие платформы, как NEM, Nxt, EOS, KickICO и другие. Каждая из них обладает своим собственным внутренним алгоритмом, позволяющим определить её уникальность.

¹⁰ Использование кодовой базы программного проекта в качестве старта для другого – [Электронный ресурс] / Википедия – свободная энциклопедия

Так же, как и в Waves, токен в Эфириуме – это цифровой актив, созданный внутри платформы, с тем лишь отличием, что процесс эмиссии токена более сложный, но при этом и более гибкий¹¹. Процесс создания токенов требует ещё написание смарт-контракта. И в связи с тем, что интеграция данного смарт-контракта в разные сервисы, биржи и криптокошельки - технический процесс, требующий автоматизации, встал вопрос минимизации времени подключения в связи с разноплановым стеком технологий. Именно тогда команда Ethereum придумала стандарты, применяемые для создания токенов. Ethereum Request for Comments (ERC) — это рекомендация для написания смарт-контрактов. Сейчас существует два основных стандарта для токенов. ERC-20 и ERC-721. Первый подходит для большинства решений. ERC-20 описывает все базовые потребности сторон, предъявляемые к токenu, и постоянно дополняется новыми правилами и рекомендациями, что делает работу разработчиков новых монет более простой и понятной. Имеется и более продвинутая версия стандарта – ERC-223, позволяющая возвращать токены со смарт-контракта, отправленные туда по ошибке. Она еще позволяет удешевлять стоимость обработки запросов, которые осуществляет смарт-контракт. По сути, в ближайшее время стандарт ERC-20 вберет в себя весь функционал ERC-223. Стандарт ERC-721 в свою очередь может быть использован для подтверждения права владения уникальными вещами ручной работы, коллекционными ценностями. Также реально использовать токен в качестве членства в закрытом клубе, проведения голосований, подтверждения прав владения активами.

Само собой кроме использования открытого кода и создания форка готового токена, или же создание на базе интеграционной платформы, примеры которой я приводил выше, есть ещё один вариант создания криптовалюты. Создание криптовалюты на основе собственного уникального блокчейн решения является самым сложным вариантом, однако такой вариант используется в том случае если команда проекта собирается внедрять новую криптовалюту в качестве нового крупного игрока на рынке.

Также при написании криптовалюты в программный код добавляется алгоритм шифрования данной криптовалюты. Алгоритмы бывают разные, и я рассмотрю самые основные из них. Они являются тем самым необходимым звеном, соединяющим майнинг с криптовалютой: именно данные алгоритмы расшифровывает майнинговое оборудование, при этом получая в качестве

¹¹ Алекс Полански. Эра криптовалюты. – М.: Издательство АСТ.

вознограждения. Данная часть включается во второй уровень стека технологий.

- Bitcoin использует алгоритм SHA-256. В связи со сложностью дешифрования данного алгоритма стандартные методы майнинга не способны выработать необходимую мощь. Для дешифрования используется оборудование - ASIC (application specific integrated circuit – интегральная схема специального назначения)
- Ethereum - DaggerHashimoto. На официальном аккаунте платформы описан следующий принцип создания: “Выгода от создания специализированного аппаратного обеспечения для алгоритма должна быть как можно меньше, в идеале до такой степени, что даже в экономике, где разрабатываются ASIC, ускорение достаточно мало, чтобы пользователям на обычных компьютерах по-прежнему было незначительно выгодно добывать их с запасной мощностью процессора”.
- Ripple (криптовалюта XRP) - ECSDA. Используемый уже в 1999 банками для более быстрого и защищенного метода совершения транзакций.
- DogeCoin - Scrypt. Раньше этот алгоритм был отличной альтернативой, когда ASIC были разработаны только для SHA256. Однако в скором времени появились Scrypt-ASIC и данный алгоритм тоже стал недоступен большинству майнеров.

Из всего вышесказанного можно понять, что большое отличие в стеках технологий у криптовалют может стать большой проблемой при интеграции. Однако тут возникает вполне логичный вопрос, каким образом данные токены добавляются в криптокошельки и биржи? Если сравнить процесс использования криптовалюты с обычными деньгами с точки зрения технологий, то вполне очевидным выводом является сложность блокчейн-технологии перед классической структурой. На основе указанной информации уже можно предположить разные варианты интеграции криптокошелька в банковскую отрасль, что подтверждает целесообразность исследования поставленной гипотезы. Как я уже выше писал, криптовалютный рынок начинает представлять из себя некое дерево, корнями которой являются блокчейн-платформы, такие как bitcoin, ethereum или waves, а криптовалюта выступает в роли веток: из нижней части вырастают разные варианты токенов со своими инновационными решениями. Либо форки, различающиеся от оригинала лишь мелкими

деталями.

Технологическая модель работы криптокошельков.

Описание криптокошелька и основная теория его функционала.

Выше я рассмотрел криптовалюту, как с точки зрения обычного пользователя, так и основную технологию, на которой криптовалюта базируется. Теперь встает логично вытекающий вопрос, как максимально удобно использовать криптовалюту, как денежную единицу. Цифровые деньги не могут просто существовать без определенного сервиса, который называется криптокошельком (электронным кошельком). Это либо программа, либо зашифрованная запись о счёте пользователя. Программа имеет удобный интерфейс, сочетающий в себе множество функционала, и может быть использована на разных цифровых носителях. Процесс проведения транзакций следующий: программа, подключается к сети блокчейн, записанной в алгоритме криптовалюты и подтверждает её легитимность. По сути, выполняет одну из задач консенсуса. А в дальнейшем вносит данные о транзакции в реестр.

В прошлой главе я упомянул о том, что криптокошельков бывает несколько видов. Сейчас рассмотрим их все подробнее. Как можно было заметить, важная деталь в работе кошелька - связь с блокчейном. И один из критериев деления криптокошельков на виды - по способу связи с системой блокчейн.

1. Hot wallet (горячий кошелёк, или же горячее хранение)

В случае горячего хранения поддерживается постоянная связь с системой. Это увеличивает скорость проведения транзакций, однако при этом увеличивается уязвимость для хакерских атак.

2. Cold wallet (холодное хранение)

Другой способ интеграции с системой при котором отсутствует постоянная связь. В противовес первому виду, лучше защищён от хакерских атак.

Следующий критерий, который я бы хотел рассмотреть - формат хранения ключей.

1. Бумажный кошелёк.

Самый первый и самый простой вариант хранения закрытых ключей. Я о нём рассказываю для понимания технических возможностей, а точнее того факта, что не обязательно иметь аккаунт в сервисах, предоставляющих возможность пользования криптовалютой для её

использования. И очевидным фактом такого кошелька является холодный вид хранения.

2. Программный кошелёк.

Тот самый вид кошельков, который очень сильно сейчас развивается, и о котором я неоднократно упоминал. В программном кошельке, как рассказывает автор книги “О Криптовалюте”, закрытый ключ шифруется с паролем на компьютере или в приложении, и появляется возможность получать и отправлять деньги через это приложение без неудобной функции импорта и исполнения, как в офлайн-кошельках. Программные кошельки, как и обычные онлайн-продукты, могут быть использованы тремя разными способами:

- приложение на компьютере.
- приложение на смартфоне.
- веб-версия приложения.

Большинство криптокошельков поддерживает первые два способа, а некоторые и все три. К примеру, такие популярные криптокошельки, которые рекомендует официальный сайт разработчиков биткоина¹², Vither, Electrum и VitPay. Более подробно некоторые из криптокошельков я рассмотрю чуть позже.

Программные кошельки бывают как с холодным типом хранения, так и с горячим.

3. Аппаратный кошелёк

Аппаратные кошельки – это компактные гаджеты, похожие на USB-накопитель, для хранения криптовалют. Высокая степень безопасности достигается за счет того, что приватные ключи доступа хранятся на этом устройстве в зашифрованном виде. Несколько уровней защиты, в том числе пин-кодом, делают его надежным.. Наиболее популярные аппаратные кошельки – Ledger Nano, Trezor.¹³ Как и бумажный кошелёк, аппаратный имеет холодный вид хранения данных.

Использование аппаратного кошелька для проведения транзакций подразумевает подключение к компьютеру. В теории аппаратный кошелёк можно назвать банковской картой в мире криптовалюты. Это физический объект, который требует для использования специальное оборудование. Однако по сравнению с банковскими картами, данные

¹² <https://bitcoin.org/ru/choose-your-wallet>

¹³ Пол Винья, Майкл Кейси. Эпоха криптовалют. Как биткоин и блокчейн меняют мировой экономический порядок. – М.: Издательство Манн, Иванов и Фербер, 2017.

на нем не являются скопированными или дублированными, и не могут быть взломаны без прямого подключения к нему.

4. Криптовалютная биржа

Биржа предоставляет возможность обмена разного рода токенов, если существует техническая поддержка конечно, в том числе на популярные государственные валюты, такие как российские рубли, американские доллары или европейское евро. Основная работа ведётся через браузер, без необходимости дополнительной интеграции кошельков. Биржа позволяет создать внутренний счёт и хранить данные на нём.

Я рассмотрел разные варианты криптокошелька для дальнейшего понимания, какие именно можно интегрировать в банковскую систему и каким образом. В прошлой главе много внимания было уделено теории криптовалюты, и из каких технических характеристик она состоит. Я упоминал о стандартах и алгоритмах шифрования. На криптокошельки данные параметры тоже имеют большое внимание. Во-первых, стандартизация криптовалюты позволяет выделить криптокошельки, которые в своём распоряжении имеют лишь определённый круг токенов. Как пример можно выделить популярный криптокошелёк MyEtherWallet (MEW), которая позволяет распоряжаться лишь криптовалютой стандарта ERC-20, а точнее написанной на базе блокчейна Ethereum. Этот факт позволяет мне сделать следующий вывод: техническая архитектура и бизнес-модель многих криптокошельков различаются, что приводит к выделению уникальных черт среди них и более кастомизированному подходу в вопросе интеграции. Если рассмотреть вопрос внедрения криптокошелька в банк с точки зрения консалтингового проекта, очевидным фактом является то, что для разных банков подойдет разная модель интеграции.

Теперь перейдём непосредственно к разбору функционала криптокошельков. Многие из приложений имеют в своём распоряжении возможности, схожие с возможностями банковских продуктов.

Несложный поиск позволил найти большое количество криптокошельков. Я выбрал из них несколько самых популярных и активно развивающихся, чтобы проанализировать их функционал. Выше я упоминал о сложности интеграции возможности работы с определенной валютой в кошелёк, следовательно у разных кошельков есть уникальный список криптовалют,

которые они поддерживают.

Продукт	Функционал	Платформы	Поддержка криптовалют
Crypterium ¹⁴	<ul style="list-style-type: none"> ● Покупка / обмен ● Получение / отправка ● Отслеживание ценности в режиме реального времени ● Онлайн оплата через телефон 	<ul style="list-style-type: none"> ● IOS 	BTC (Bitcoin) ETH (Ethereum) LTC (Litecoin) CRPT (Crypterium)
Blockchain ¹⁵	<ul style="list-style-type: none"> ● Получение / отправка ● Покупка / продажа / обмен ● Двухфакторная аутентификация 	<ul style="list-style-type: none"> ● IOS ● Android ● Web 	BTC, ETH, BCH (Bitcoin cash)
Coinbase ¹⁶	<ul style="list-style-type: none"> ● Покупка / обмен (через биржу) ● Получение / отправка 	<ul style="list-style-type: none"> ● IOS ● Android 	BTC, BCH, ETC (Ethereum Classic), ETH, LTC + ERC-20 токены

¹⁴ <https://crypterium.com/>

¹⁵ <https://www.blockchain.com/ru/wallet>

¹⁶ <https://wallet.coinbase.com/>

	(через биржу) <ul style="list-style-type: none"> ● Хранение ● Отслеживание ценности в режиме реального времени 		
Trust Wallet ¹⁷	<ul style="list-style-type: none"> ● Покупка / обмен ● Получение / отправка ● Двухфакторная аутентификация 	<ul style="list-style-type: none"> ● IOS ● Andr 	BTC + ERC-20, ERC-721 и ERC-223

Очевидным фактом является довольно обычный набор функционала у продуктов, однако есть несколько инноваций в данной сфере, о которых я бы хотел рассказать. Во-первых, как можно заметить компании стараются внедрять двухфакторную аутентификацию. Приложение, идеей основного продукта которой является безопасной, улучшает именно данную зону ответственности. Во-вторых, у продукта Crypterium есть возможность онлайн оплаты через карточку / телефон (бесконтактные платежи - технология NFC) в местах, где принимают оплату Google / Apple pay. Механизм оплаты происходит через автоматический обмен криптовалюты на USD (доллар) / EUR (евро). Этот факт позволяет сделать вывод о возможностях введения популярного функционала, который уже давно интегрирован в банковские продукты.

Техническая архитектура криптокошелька

Для внедрения функционала криптокошелька в банковскую отрасль необходимо выявить слои архитектуры обоих объектов, участвующих в интеграции. В прошлых параграфах было рассказано про техническую часть

¹⁷ <https://trustwallet.com/>

продукта и предоставляющий функционал. В этом параграфе я попробую объединить данную информацию в единую систему.

Начну с верхнеуровневого изображения концепции работы блокчейн-системы. Как можно видеть (Рис.1), концепция блокчейн системы заключается в механизме, который позволяет работать этой системе - майнинге, в который включается хэширование данных. Далее блокчейн состоит из алгоритмов консенсуса, регулирующий взаимоотношение между пользователями системы. Свойства блокчейна показывают основную философию данной технологии, которая является базой для её уникальности. В данном графике я представил криптовалюту, как созданные на основе технологии системы ценностей, однако как мы знаем, это лишь один из вариантов развития технологии. Обязательно указаны варианты работы блокчейна, а точнее деление на “публичный” и “приватный”. И в заключение примеры использования. Я указал лишь те, которые имеют ценность в данном исследовании.

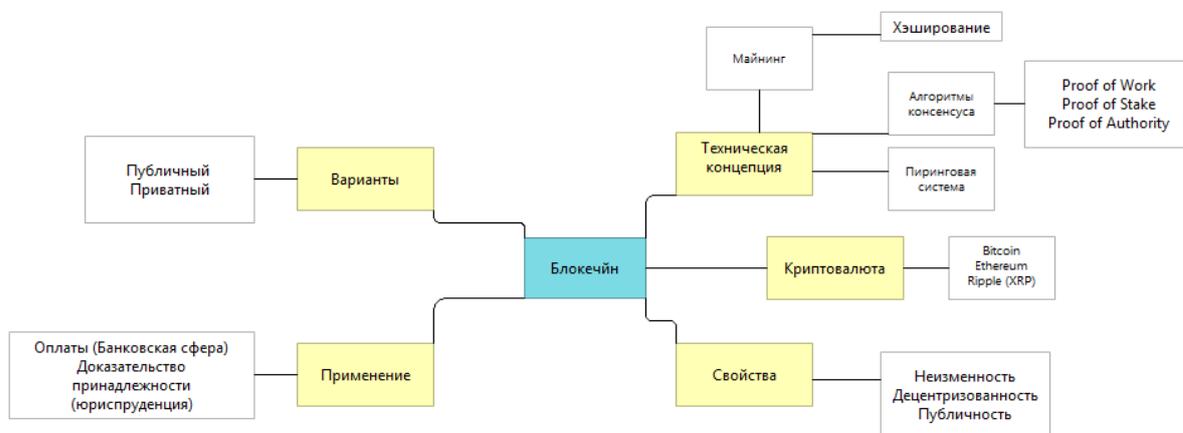


Рис. 1.

Данный этап исследования реализован с помощью оценки теоретической части технической составляющей и модели работы отдельных частей общего продукта (технология блокчейн; криптовалюта; криптокошелек) и дальнейшего моделирования архитектуры данных частей при помощи программы ArchiMate.

Разобравшись в общей модели блокчейна я создал общую архитектуру блокчейн-технологии. Это первый этап в исследовании архитектуры работы криптокошелька (Рис.2).

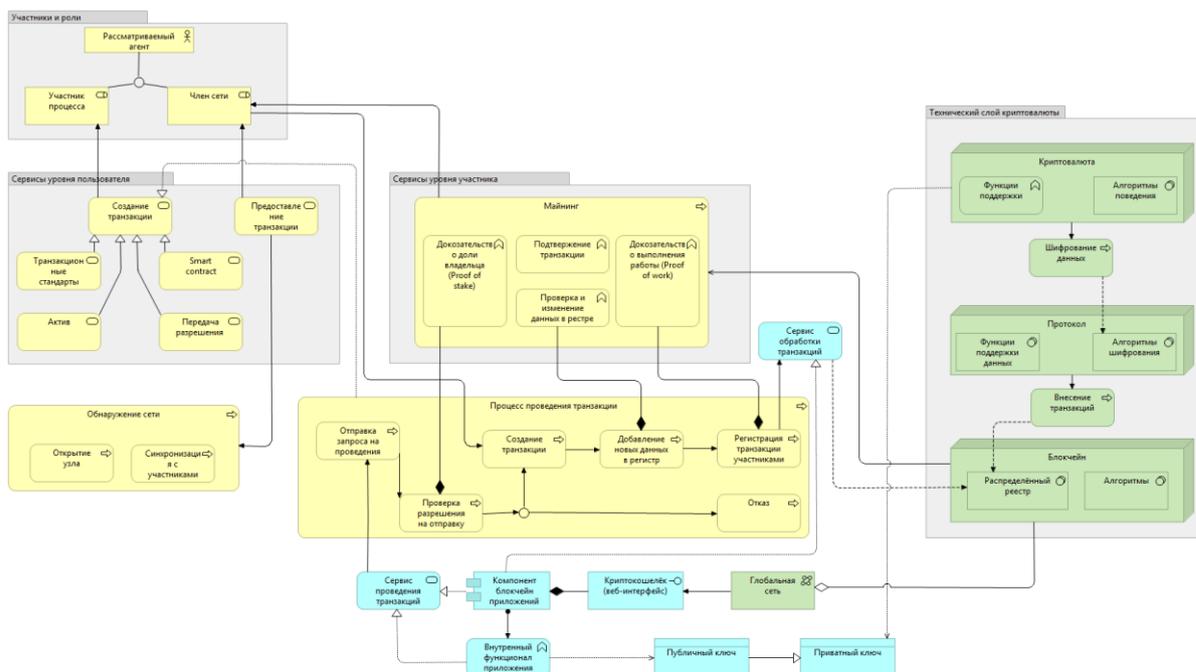


Рис. 2.

В группе “технический слой криптовалюты” показана уже рассмотренная трёхслойная модель: блокчейн - протокол - криптовалюта. Исследовав открытый исходный код таких криптокошельков, как “Coinbase” и “Blockchain” и “Trust Wallet” я выявил сходства в написании системы связей с общей блокчейн-системой. Во-первых, связь устанавливается прямая, на основе того, с какими криптовалюта работает криптокошелёк. Это может быть как Ethereum, Bitcoin, так и другие блокчейны. Во-вторых, у криптокошельков существует документ со списком криптовалют и хранение их идентификационного номера. Обращаясь к этому документу приложение получает доступ к общей базе транзакций блокчейна, где может принимать участие в качестве посредника для проведения операций.

Следующий этап, детальное рассмотрение архитектуры криптокошелька (Рис. 3).

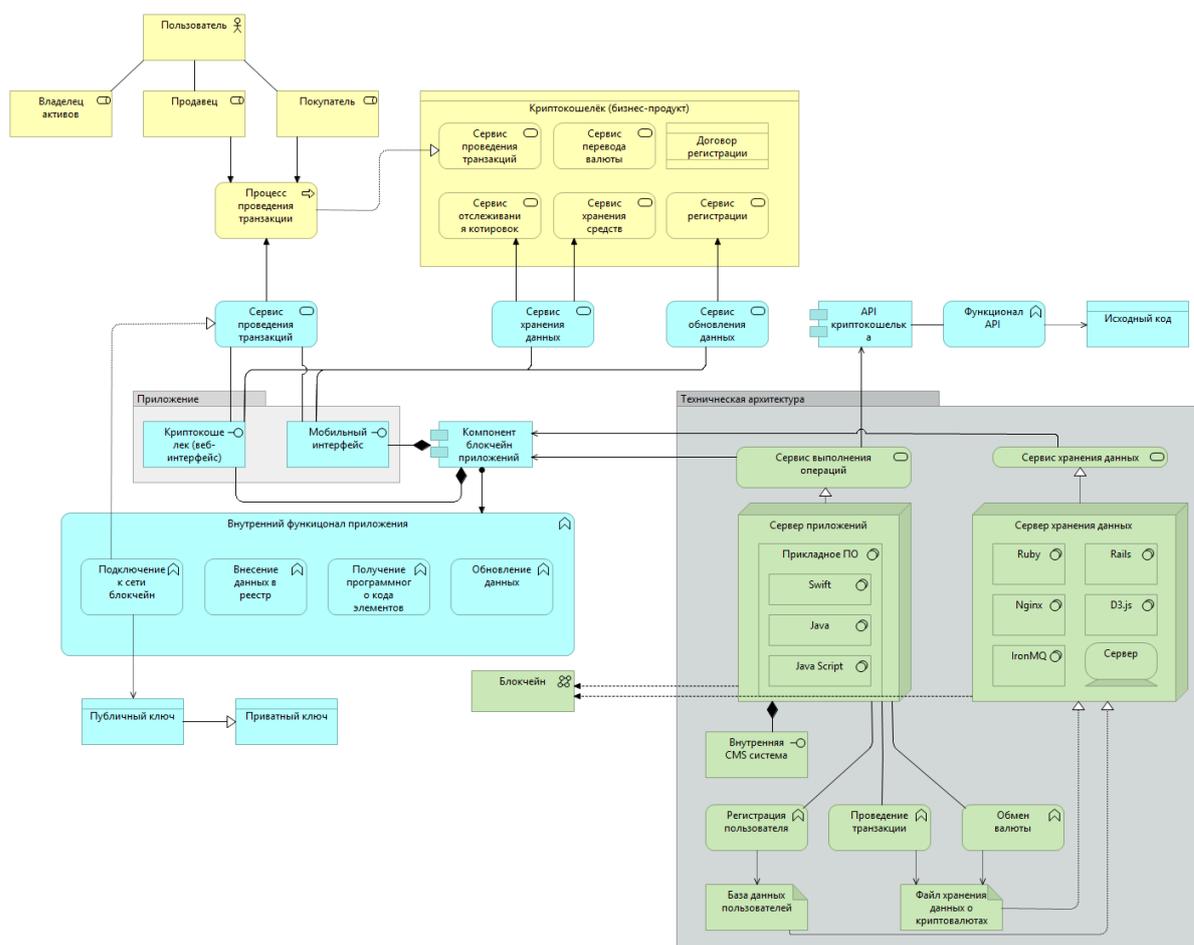


Рис. 3.

Бизнес уровень

При составлении архитектуры я добавлял только процессы, которые непосредственно рассматриваю в данном исследовании. Замечу, что процессов и функций у продукта намного больше, чем представлено в модели. Пользователь продукта может выступать в роли как покупателя, так и продавца. Основной процесс, на основе которого я планирую в дальнейшем рассматривать варианты интеграции - проведение транзакции (перевод средств от одного участника другому).

Уровень приложений

В уровне приложений рассматриваются основные сервисы (функционал приложений), которые были выявлены в прошлом параграфе. Замечу, что здесь показаны только два вида интерфейса: “веб-приложение” и “мобильный интерфейс”. Я не рассматривал аппаратный кошелёк, потому что внедрение технологии рассматриваю только на уровне онлайн-

приложений, как дополнительный сервис к онлайн-банкингу. Ещё одним важным моментом является компонент блокчейн-приложений. Я выделил именно такую общую структуру, так как это является в более долгосрочной перспективе путём для выстраивания крупной архитектуры продуктов, на основе технологий блокчейн, которые я рассматривал в первой главе.

Технический уровень

Основной стек технологий, которым пользуются разработчики приложений криптокошельков указан на данном графике. Хочу отметить важность в использовании профессиональных баз данных, так как данное приложение имеет в первую очередь характер хранения информации. Именно поэтому я поделил узлы (исполнитель ключевых операций в технологическом слое) на две части. Вторая - сервер приложений, включает в себя всю информацию по программному коду приложения, который позволяет ему работать. В ней также присутствует непосредственно алгоритм работы с блокчейном. Как я упоминал выше, в базах данных хранится информация по подключению к распределённому реестру, а в программном коде приложения разработан алгоритм выполнения данного процесса. Это означает, что данные две части работают взаимосвязано. Ещё дополнительно я бы хотел отметить существование API подключения к общей сети криптовалюты. К примеру, у такого криптокошелька, как Blockchain существует своя API¹⁸, на основе которой компании могут реализовать свой собственный продукт-криптокошелёк. Они предлагают внедрение таких сервисов, как: данные о реестре¹⁹: “Запрос данных JSON по блокам и транзакциям”; алгоритмы запросов²⁰; Websockets²¹, которые позволяют получать в режиме реального времени информацию о возникновении новых данных о транзакциях в реестре для обновления информации. Данная информация важна, так как это позволяет получить ещё один дополнительный способ внедрения нового продукта в банковскую архитектуру.

И последняя модель, которую я бы хотел рассмотреть на данном этапе, показывает самый последний уровень в данной архитектуре: модель процесса проведения транзакций (Рис. 4)

¹⁸ <https://www.blockchain.com/ru/api>

¹⁹ https://www.blockchain.com/ru/api/blockchain_api

²⁰ <https://www.blockchain.com/ru/api/q>

²¹ https://www.blockchain.com/ru/api/api_websocket

Эта модель показывает взаимосвязь пользователя с продуктом и его уровнем приложений. А также в данной модели я более детально рассмотрел сам процесс проведения транзакции. Он приводится в исполнения после события, который реализует покупатель “подача заявления для выполнения транзакции”. По сути это техническая передача валюты от одного аккаунта на другой.

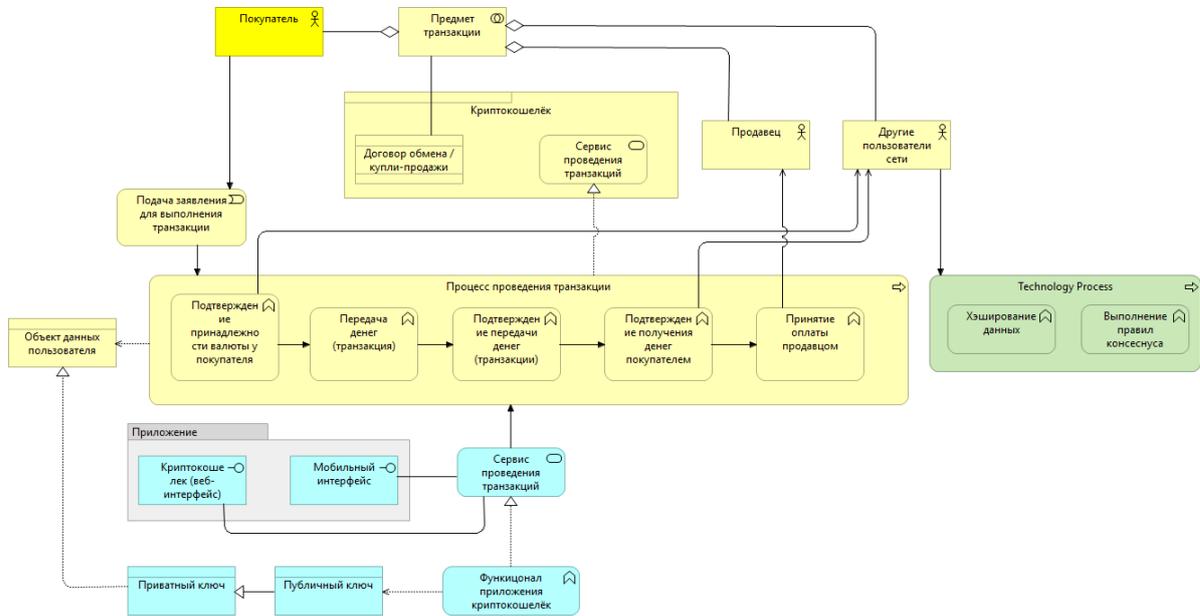


Рис. 4.

Однако внутри данного процесса есть ещё участники, другие члены сети, которые на техническом уровне подтверждают возможность проведения транзакции. Основным проблемным моментом в данном процессе являются последние два этапа. Я рассмотрел подробно внутренний функционал нескольких криптовалют, и некоторые из них требуют ручного подтверждения получения транзакции, к примеру, “MyEtherWallet”. А точнее, средства не будут зачислены на счет пользователя, если он самостоятельно не добавит данные из подтвержденной транзакции к себе в кошелёк.

Интеграция технологии криптокошелька в классическую банковскую систему.

Техническая архитектура банковской индустрии.

Архитектура банковского предприятия в этом исследовании будет показана на самом базовом уровне, без излишних дополнительных элементов (Рис. 5)

Модель показывает разделение архитектуры на три основных слоя, аналогично архитектуре криптокошелька. Я рассмотрел в данной модели процессы и продукт, по формату схожий с процессами, рассмотренными в прошлых моделях.

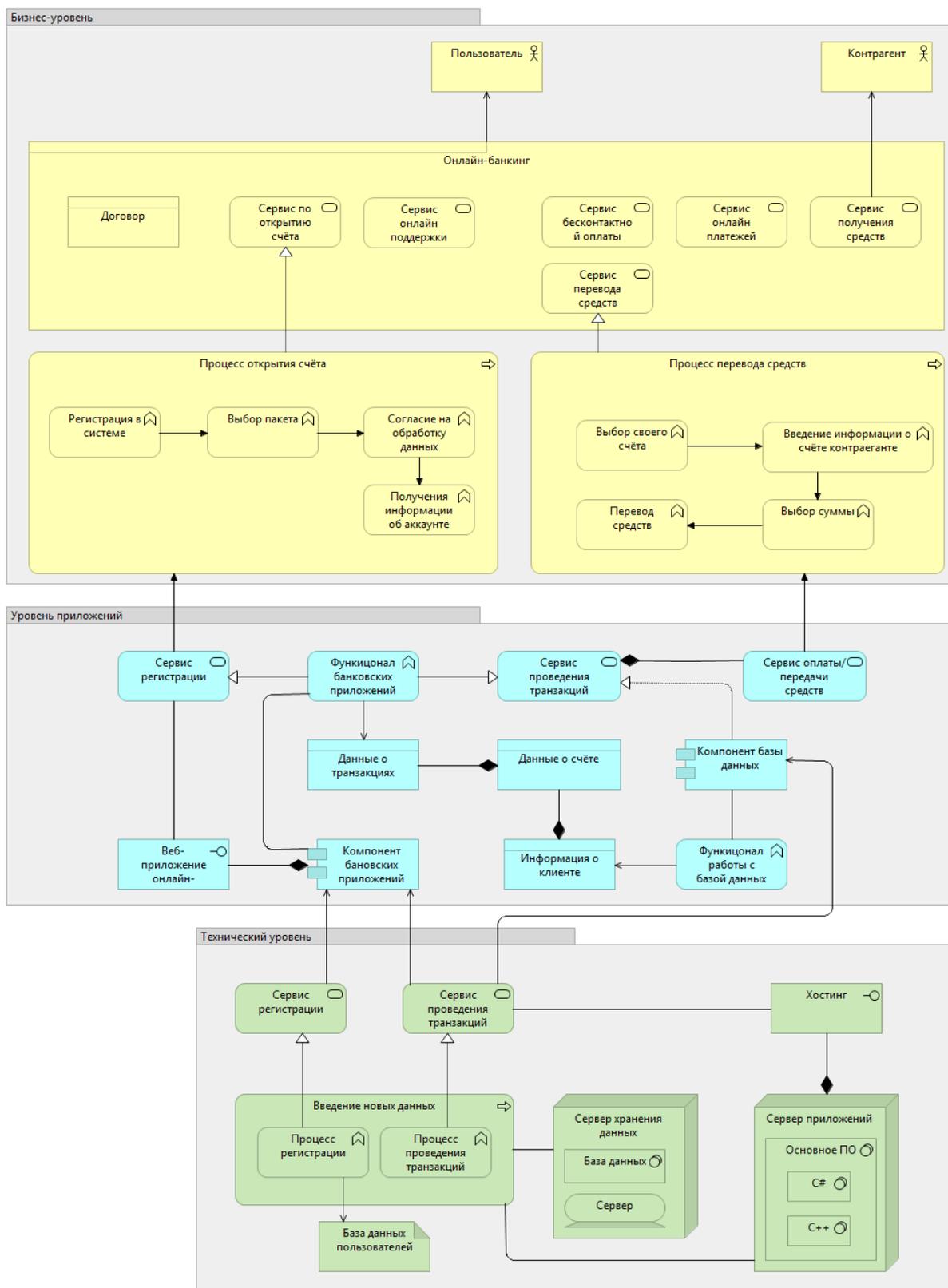


Рис. 5.

Продукт - онлайн-банкинг является основным продуктом, который будет являться основным элементом принимающим в себя дополнительный технический функционал. Он позволяет реализовывать следующие два

процесса: регистрация и проведение транзакции (аналогично функционалу криптокошелька). Замечу, что как и в прошлых моделях, продуктов и бизнес-процессов в банковской отрасли существует намного больше, однако они не имеют ценности для данного этапа исследования. Процесс проведения транзакции через банковский сервис схож по технической составляющей с технологией блокчейн и архитектурой криптокошелька. При выполнении процесса пользователям происходит отправка запроса через веб-интерфейс в базу данных банка, где хранится вся информация об аккаунте пользователя. В данном случае третьим лицом, подтверждающим возможность выполнения транзакции является непосредственно банк. Однако разница в данном процессе между рассматриваемыми двумя технологиями в том, что у банка хранится информация о средствах пользователя в прямом виде, без дополнительных факторов. То есть происходит обычная проверка на разницу в стоимости выполнения транзакции. В блокчейне же данный алгоритм работает по-другому. На техническом уровне проверяется не наличие у пользователя определённого количества средств у пользователя, а в первую очередь происходит проверка на существования данных средств в общей базе данных, а точнее реестре блокчейна.

Варианты внедрения сервисов криптокошелька в банковскую систему.

Как я уже писал выше, варианты внедрения будут варьироваться от требований и возможностей бизнеса. Я попробую предположить самые возможные в плане реализации варианты. Все последующие размышления основаны на указанном выше исследовании бизнес-функций и технических требований обеих предметов интеграции.

В первую очередь рассмотрим самый очевидный вариант внедрения технологии в архитектуру банка: создание собственного дополнительного слоя технологии, работающей с криптовалютой.

Дополнение к готовому продукту

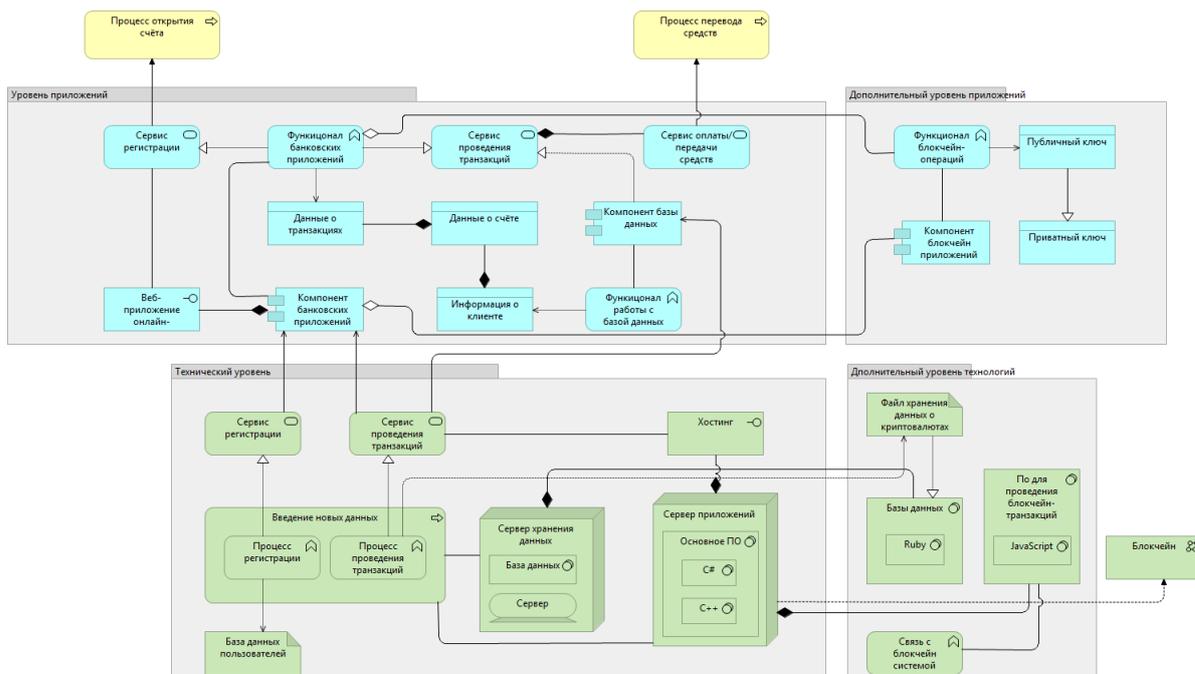


Рис. 6.

В данном варианте интеграции отсутствует изменение бизнес слоя архитектуры. Основные изменения будут происходить на уровне приложений и техническом слое. С точки зрения пользователя, он получает возможность работы с криптовалютами. Эта возможность на уровне приложений будет предоставляться аналогично обычному функционалу банковского продукта. Приложение “онлайн-банкинг” будет являться основным веб-интерфейсом в данном случае (без внедрения дополнительного приложения). Основной сложностью данного внедрения с точки зрения единой структуры является вопрос безопасности. Алгоритмы шифрования криптокошелька и внутренних данных отличается от банковских. Следовательно трудностью будет являться интеграция новых пользовательских данных в общую базу данных. И конечно в данном случае не может идти речи об анонимности при использовании функционала, предоставляющего технология блокчейн.

И на данном этапе встает вопрос, как можно добавить в банковскую продуктовую линейку возможность использования криптовалюты без нарушения “блокчейн-философии”.

Создание нового криптокошелька

В данном случае создается новый продукт, который является отдельной частью компонента банковских приложений. Внедрение в архитектуру я произвел с учетом интеграции сервисов между с собой среди двух продуктов: “онлайн-банкинг” и “криптокошелёк”.

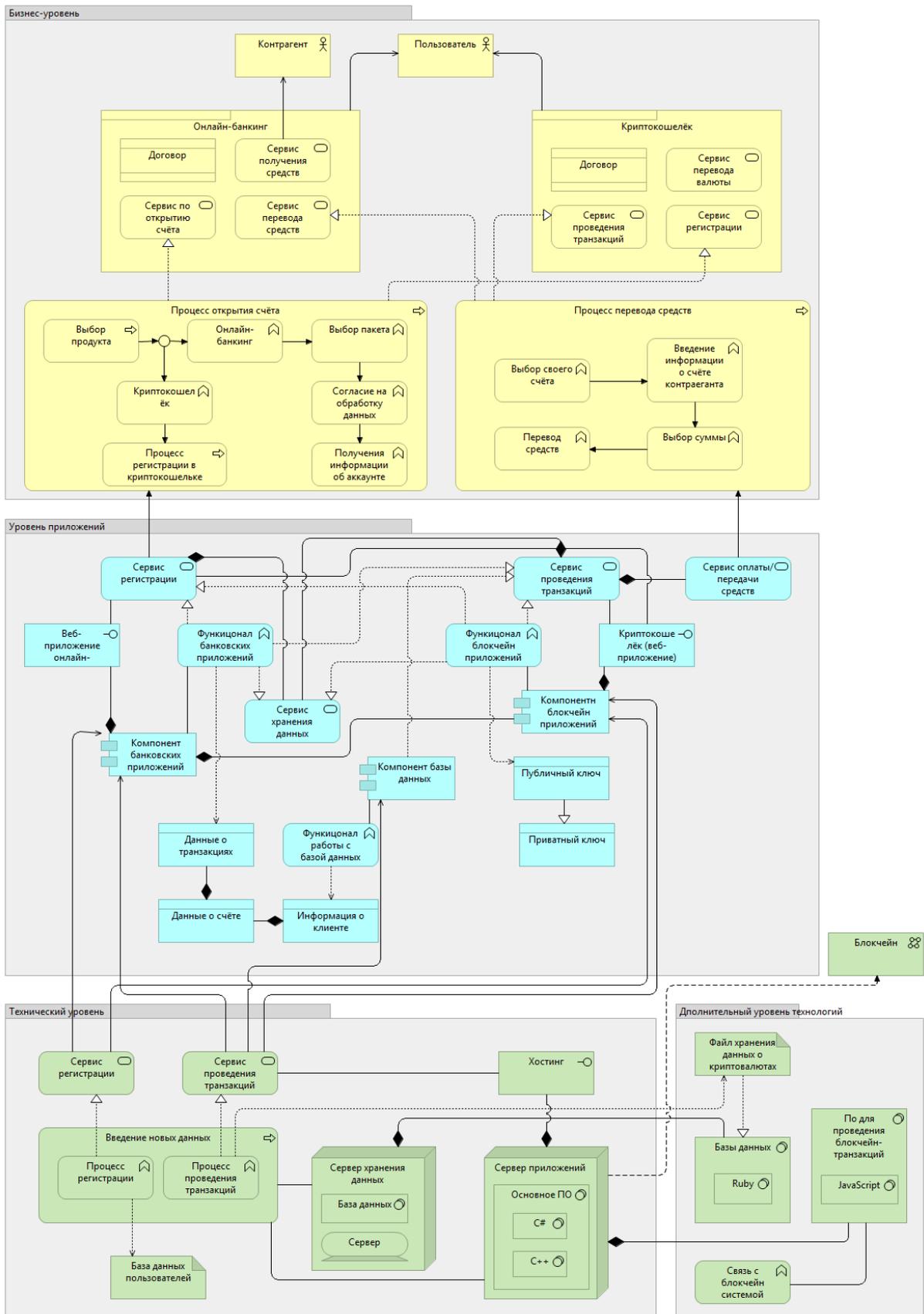


Рис. 6.

Алгоритм дополнения технического слоя не сильно отличается от прошлого рассмотренного варианта. Однако сильное изменение видно на уровне приложений. Пользователь, в сравнении с прошлым пунктом, взаимодействует с двумя приложениями. Они оба должны быть интегрированы с единой системой, в которой записывается общая информация о пользователе и о транзакциях, проводимых как через классическую систему, так и через блокчейн.

Данный вариант позволяет использовать единую базу данных об аккаунтах пользователей. Однако он довольно сложен с точки зрения программирования нового приложения и намного сильнее подвержен внешним атакам.

Отсюда возникает следующий вопрос, можно ли внедрить возможность использования технологии блокчейн и работы с криптовалютой другим способом. Способом, который будет по сути аналогичен новому криптокошельку, однако при этом являться частью компонента банковских приложений, дающий возможность соединения баз данных отдельных приложений в единое целое. Ответить на этот вопрос может упомянутый функционал в прошлой главе - API криптокошелька.

Использование API

Этот вариант позволяет банку внедрить уже готовое коробочное решение криптокошелька, изменив визуальные и внешние характеристики существующего продукта. Выбор из представленных на рынке решений и его дальнейшее внедрение в архитектуру позволит банку получить алгоритмы выполнения запросов и работы с сетью блокчейн технологии и уже интегрированными криптовалютами.

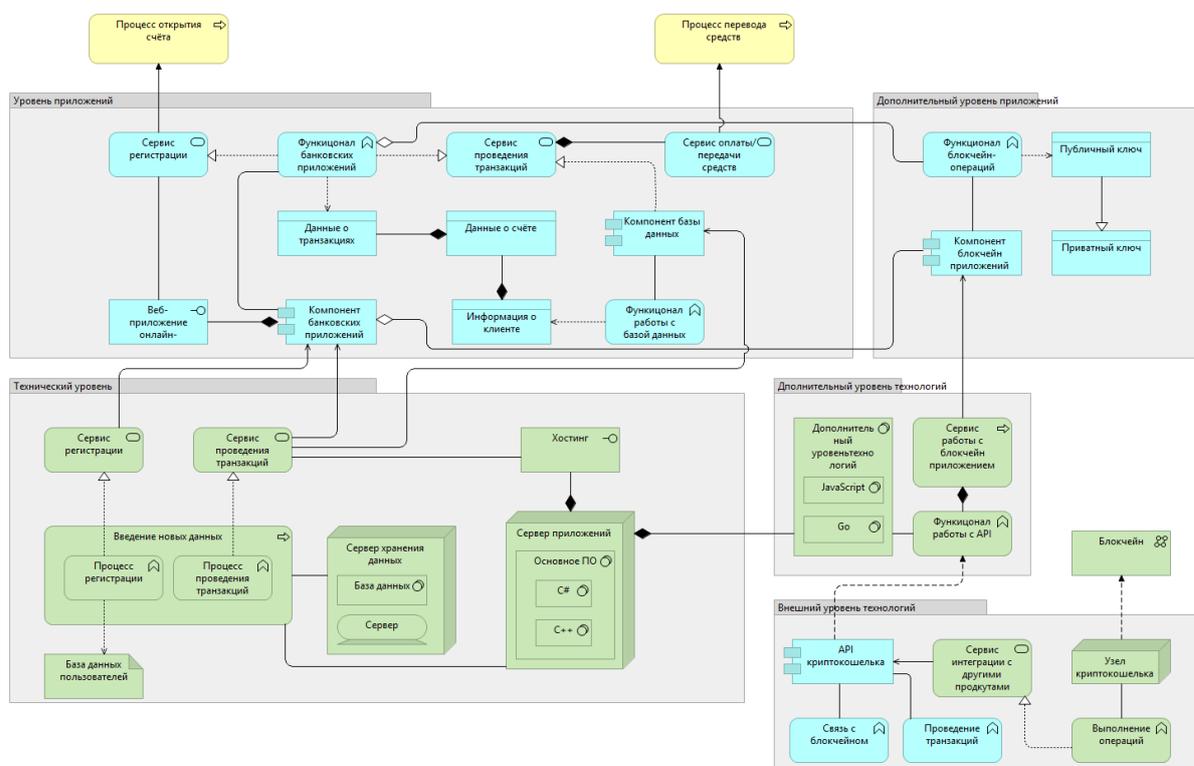


Рис. 7.

Основной минус данного варианта - ограниченность в нововведениях. Банк должен будет подстраиваться под изменения в API у исходного продукта, и работать лишь с теми активами, которые технически поддерживает данная компания. Однако это позволяет получить алгоритмы запроса и добавление уже зашифрованной информации в базу данных, при этом не нарушая принципы блокчейна.

Для реализации данного внедрения необходимо добавить на программном уровне во внешней части дополнительный уровень приложений, позволяющий пользователям взаимодействовать с функционалом блокчейн-приложений. И подключить его через API к выбранному готовому криптокошельку. Процесс регистрации в сервисе остаётся непосредственно на банке, и база данных пользователей тоже не внедряется во внешние сервисы. Однако в данном же случае у банка нет прямого доступа к транзакциям своего пользователя, их реализация происходит как раз через API. Этот вариант внедрения отличный для таких банков, как “Модульбанк”, банк “Точка”, “Рокетбанк” и другие, которые не являются крупными игроками на рынке, однако имеют большой пользовательский потенциал на внедрения технологии и работе с новым развивающимся рынком криптоплатежей.

Заключение

Проведение исследования и поиск возможных вариантов интеграции сервисов криптокошелька позволило выявить итоговый вариант архитектуры банковской отрасли, а точнее конкретного его продукта “онлайн-банкинг”. На основе вышесказанного можно сделать вывод, что при выявлении необходимых критериев, существует разный, соответствующий потребностям, способ внедрения новой технологии. Замечу, что я интегрировал криптокошелёк в банковскую отрасль с уже готовым функционалом и сервисом, который был выявлен в результате теоретического исследования. Однако банк, который собирается использовать технологию может добавлять новую структуру, функционал, стек технологий и другие необходимые параметры. Неизменным остаётся обязательно формат взаимодействия банковских алгоритмов технического слоя и слоя приложений с технической стороной технологии блокчейн. Рассмотренные варианты внедрения предлагают компаниям готовое решение и ответ на вопрос, какие дополнительные слои архитектуры необходимо внедрить в банковскую структуру. Три разных направления имеют свои положительные стороны и соответственно недостатки. Выбор того или иного варианта зависит от критериев необходимости, поставленных банком.

Используемая литература

Книги

- Алекс Полански. Эра криптовалюты. – М.: Издательство АСТ. – 247 с.
- Грекул В.И., Коровкина Н.Л., Левочкина Г.А. Проектирование информационных систем. – М.: ИНТУИТ, 2012
- Джулиан Хосп. О криптовалюте просто. Биткоин, Эфириум, блокчейн, децентрализация, майнинг, ICO & CO. – М.: Издательство Питер, 2019. – 121 с.
- Мелани Свон, Блокчейн. Схема новой экономики. – М.: Издательство Олимп-Бизнес, 2017. – 190 с.
- Пол Винья, Майкл Кейси. Эпоха криптовалют. Как биткоин и блокчейн меняют мировой экономический порядок. – М.: Издательство Манн, Иванов и Фербер, 2017. – 512 с.

Интернет-источники

Evolution of blockchain technology [Электронный ресурс] / Deloitte – свободные аналитические данные. – URL:

<https://www2.deloitte.com/insights/us/en/industry/financial-services/evolution-of-blockchain-github-platform.html> (Дата обращения: 17.05.2019)

What is the history of blockchain technology? [Электронный ресурс] / Quora – свободные научные публикации. – URL: <https://www.quora.com/What-is-the-history-of-blockchain-technology> (Дата обращения: 19.04.2019)

Blockchain Generations Explained in 2019 | Blockchain History [Электронный ресурс] / Meetnoor – новостной интегратор. – URL: https://meetnoor.com/blockchain-generations/#Blockchain_Technology_Blockchain_History (Дата обращения: 19.04.2019)

Blockchain Architecture Basics: Components, Structure, Benefits & Creation [Электронный ресурс] / MLSdev – веб-интегратор технологий. – URL: <https://mlsdev.com/blog/156-how-to-build-your-own-blockchain-architecture> (Дата обращения: 4.05.2019)

Understanding Web 3—A User Controlled Internet [Электронный ресурс] / Coinbase – свободная новостная платформа. – URL: <https://blog.coinbase.com/understanding-web-3-a-user-controlled-internet-a39c21cf83f3> (Дата обращения: 10.05.2019)

Статьи

Richard Meszaros, Diana Adachi, Hanif Dharamsi, Burak Yetiskin. Paul Thomas, HOW BLOCKCHAIN TECHNOLOGY CAN REVOLUTIONIZE BANKING // Accenture. – М., 2016.

Dr Garrick Hileman, Michel Rauchs. GLOBAL CRYPTOCURRENCY BENCHMARKING STUDY // Cambridge Centre for Alternative Finance. – М., 2017

Davor Svetinovic. Towards Reference Architecture for Cryptocurrencies: Bitcoin Architectural Analysis. М.: Conference: 2014 IEEE International Conference on Internet of Things(iThings), and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom)

Andreas Ellervee. A Reference Model for Blockchain-Based Distributed Ledger Technology // UNIVERSITY OF TARTU Institute of Computer Science Software Engineering Curriculum – М., 2017