
# ДЕЦЕНТРАЛИЗОВАННАЯ СЕТЬ ОБМЕНА И ХРАНЕНИЯ ИНФОРМАЦИИ «МАСТЕРЧЕЙН»

Версия 1.1

WHITEPAPER

Ассоциация развития финансовых технологий
Москва, 2017

| | |
|---|---|
| А. Архипов | alexey.arkhipov@fintechru.org |
| Т. Билык | bta2@cbr.ru |
| А. Благирев | alex@open.ru |
| Д. Булычков | dabulychkov2@sberbank.ru |
| М. Григорьев | grigorievma@cbr.ru |
| К. Ивкушкин | kvivkushkin@sberbank.ru |
| П. Каламбет | p.kalambet@qiwitech.ru |
| Е. Кирцова | e.kirtsova@qiwi.com |
| Р. Скляр | roman.sklyar@open.ru |
| В. Сорокин | sorokinve@cbr.ru |
| А. Трошичев | alexey.troshichev@fintechru.org |



Ассоциация развития финансовых технологий
Москва, 2017

# СОДЕРЖАНИЕ

# 1. ЦЕЛЬ ДОКУМЕНТА

Документ декларирует основные принципы работы распределенной системы **Мастерчейн**, создаваемой на базе технологий распределенных реестров и структуры данных типа *blockchain* (*блокчейн*), а также области его применения. Документ рассчитан на подготовленных пользователей, владеющих общей терминологией распределенных реестров, техническими терминами и определениями, применяемыми для описания и формализации протоколов децентрализованных сетей.

Документ подготовлен в рамках рабочей группы «Ассоциации Развития Финансовых Технологий» (далее АФТ) и является собственностью АФТ. Документ может дополняться и модифицироваться в связи с изменениями законодательства Российской Федерации, нормативных актов Банка России, развитием существующих технологий распределенных реестров.

В документе последовательно изложены:

1. Предпосылки. Сформулированы цели создания **Мастерчейн**.
2. Определение требований к технологической реализации.
3. Обзор существующих продуктов (которые представлены участниками АФТ), которые могут быть оптимизированы при использовании технологии распределенных реестров, то есть работать на базе **Мастерчейн**.

Разработка данного документа осуществлялась посредством изучения и анализа существующих протоколов работы распределенных реестров, опыта их эксплуатации.

# 2. ОСНОВНЫЕ ПРОБЛЕМЫ И ПРЕДПОСЫЛКИ

На текущий момент на российском рынке отсутствуют стандартные и регулируемые распределенные реестры, что затрудняет легальное использование этой технологии участниками. При этом участники АФТ заинтересованы в развитии данной технологии и ее использовании в собственных продуктах.

Таким образом, основной предпосылкой работы над **Мастерчейн** является необходимость разработки решения для финансового рынка, где участники могли бы реализовывать свои проекты на базе распределенных реестров (блокчейн) в среде, соответствующей требованиям российского законодательства, с использованием современных решений, совместимых с наиболее распространенными инфраструктурами существующих распределенных реестров.

# 3. ОПРЕДЕЛЕНИЕ

**Мастерчейн** – это одноранговая сеть с управляемым доступом, взаимодействие узлов которой происходит на базе модификации протокола *Ethereum*. **Мастерчейн** позволяет производить безопасную запись информации в распределенный реестр, копии которого находятся на каждом узле сети.

# 4. ГЛОССАРИЙ

**Распределенные реестр** – структура данных, нефиксированное множество копий которой может прийти к окончательно консистентному состоянию (eventual consistency), используя заданный алгоритм консенсуса.

**Сеть с управляемым доступом** – сеть с централизованным управлением доступом к сети для узлов.

# 5. ПРЕДПОСЫЛКИ

Предпосылками создания **Мастерчейн** являются следующие ограничения, присутствующие в финансовых экосистемах, в том числе на национальном уровне:

1. Существующая система посредников, обеспечивающих доверие при совершении финансовых операций, не позволяет качественно повысить скорость проведения операций и снизить транзакционные издержки.

2. Сложность обеспечения процедур аудита и управления рисками из-за фрагментации данных о проведенных финансовых операциях.
3. Отсутствие технических стандартов в части применения технологии распределенных реестров препятствует интеграции бизнес-процессов финансовых организаций и используемых ими данных.

Указанные факторы сильно ограничивают возможности внедрения новых финансовых технологий участниками финансового рынка и приводят к неравномерному распределению доступа к ним среди заинтересованных сторон. В том числе выявленные ограничения снижают возможность получения актуальной информации, существенной для принятия управленческих решений, что, в свою очередь, способствует возникновению недобросовестных практик и повышает риски проведения мошеннических операций для финансового рынка в целом.

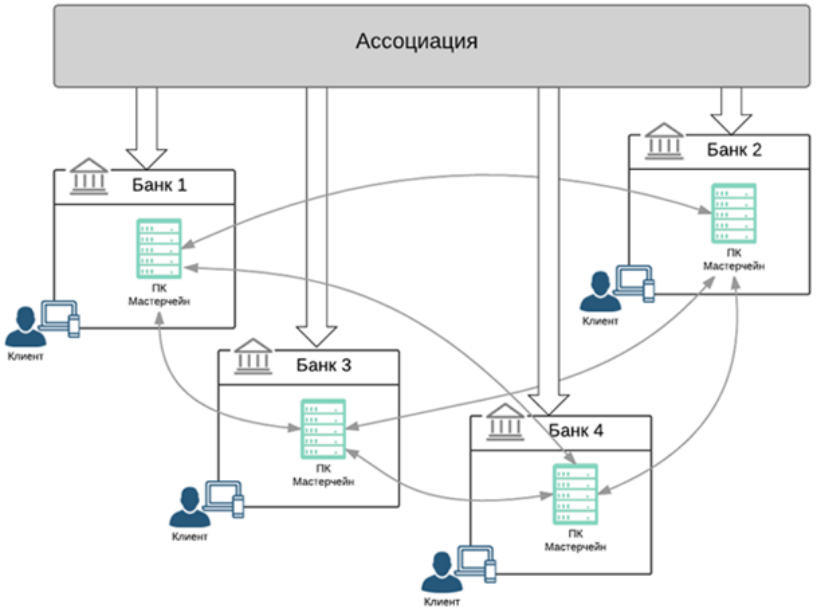
Для решения описанных проблем предлагается создать единую национальную сеть обмена и хранения финансовой информации с использованием технологии распределенных реестров (далее **Мастерчейн**) и предоставить возможность автоматизации процесса совершения финансовых операций для участников сети с использованием встроенной логики принятия решений (далее смарт-контракт).

# 6. ПРИНЦИПЫ ПОСТРОЕНИЯ

Ключевые принципы построения **Мастерчейн**:

1. Распределенный реестр **Мастерчейн** не хранит данные, требующие особого режима хранения (данные, охраняемые коммерческой тайной, персональные данные, секретные данные и т.п.).
2. Юридическая значимость (в рамках российской юрисдикции) информации, обрабатываемой в **Мастерчейн**.
3. Отсутствие технической необходимости в доверенных посредниках.
4. Поддержка программируемых контрактов (смарт-контрактов).
5. Отсутствие единой точки отказа.
6. Независимый учет ресурсов, затрачиваемых участниками на поддержку работы системы.
7. Возможность масштабирования (по количеству участников и транзакций).

## 6.1. СХЕМА ВЗАИМОДЕЙСТВИЯ




Финансовые организации, входящие в Ассоциацию, используют **Мастерчейн** для своих бизнес-процессов.

## 6.2. ПЛАТФОРМА

При формировании требований к платформе использовался опыт существующих распределенных реестров.

Требования к платформе, значимые для решаемой задачи, организуются в три группы:

1. Эксплуатационные;
2. Безопасности;
3. Функциональные.

### 6.2.1. ЭКСПЛУАТАЦИОННЫЕ ТРЕБОВАНИЯ

1. Масштабируемость по количеству узлов. Рост количества узлов не влияет на сложность алгоритма консенсуса платформы.
2. Поддержка режима распределенной системы, когда все нижеперечисленные требования одновременно невыполнимы:
   - Сетевая связность безотказна;
   - Скорость передачи информации постоянна;
   - Сеть безопасна (трафик не может модифицироваться третьей стороной);
   - Топология сети постоянна;
   - Централизованное администрирование;
   - Все узлы и все каналы связи идентичны;
   - Существуют универсальные для всей системы часы.
3. Опыт массового использования платформы в интернете без управления доступом к системе, с открытием исходных кодов.

Скорость не рассматривалась как важное эксплуатационное требование, так как скорость в условиях системы без централизованного управления (распределенной) и при неопределенном количестве участников эффективно управляться не может.

### 6.2.2. ТРЕБОВАНИЯ К БЕЗОПАСНОСТИ

1. Доказательство аутентичности цепочки. Однозначный алгоритм для единственно верной версии РР.
2. Отсутствие влияния данных внутри цепочки на логику алгоритма консенсуса.
3. Возможность расчета цены компрометации системы с высокой точностью.
4. Управляемый доступ узлов к сети.
5. Использование российских сертифицированных алгоритмов криптографической защиты информации.

### 6.2.3. ФУНКЦИОНАЛЬНЫЕ ТРЕБОВАНИЯ

1. Поддержка возможности создания в рамках сети новых экземпляров программного кода, выполнение которых влечет за собой какие-либо события (смарт-контракты).
2. Учет работы валидаторов (майнинг).
3. Управляемый доступ к сети.

### 6.2.4. ОПРЕДЕЛЕНИЕ КОМПРОМЕТАЦИИ

Платформа считается скомпрометированной, когда возможно хотя бы одно из следующих событий:

1. Умышленное изменение данных в РР, по которым сеть уже пришла к консенсусу.
2. Одновременное существование противоречивых версий РР без однозначного признака, позволяющего выбрать верную.

## 6.3. ЮРИДИЧЕСКАЯ ЗНАЧИМОСТЬ

Юридическая значимость достигается через соответствие N63-ФЗ «Об электронной подписи» от 06.04.2011, в частности, криптографические преобразования, описанные в ГОСТ, реализуются СКЗИ, прошедшими соответствующую сертификацию.

## 6.4. ВИДЫ РАСЧЕТНЫХ ЕДИНИЦ

**Технологические расчетные единицы (TPE)**. Используются для учета работы по обработке транзакций (технической комиссии). Создаются валидаторами в процессе создания блоков.

**Специализированные расчетные единицы**. Используются для операций с ценностью. Создаются в рамках смарт-контрактов, управляемых регулятором.

## 6.5. ВСПОМОГАТЕЛЬНЫЕ СИСТЕМЫ

Вспомогательные системы используют распределенный реестр для решения следующих классов задач:

1. Ускорение проведения транзакций.
2. Обработка информации, требующей специального режима обращения (персональные данные, платежная информация).
3. Мониторинг и диагностика состояния сети.
4. Интеграция со сторонними системами автоматизации.
5. Интеграция с другими распределенными реестрами через поддержку протокола *Interledger*.

## 6.6. СИСТЕМА ВОЗНАГРАЖДЕНИЯ

В ПК **Мастерчейн** реализован механизм технических комиссий за транзакции и выполнение смарт-контрактов, аналогичный механизму, реализованному на платформе Ethereum.

Для выполнения каждой транзакции (в том числе, вызывающей исполнение смарт-контракта) существует техническая комиссия, выражаемая в TPE. Для вычисления технической комиссии используется абстрактная единица, называемая *газом*. *Газ* – это единица измерения ресурсов, необходимых для обработки транзакции и записи ее в РР. Единице газа соответствует заданное администратором узла количество TPE. Соответственно, минимально необходимые затраты на транзакцию вычисляются умножением количества необходимого газа на количество TPE, соответствующее единице газа (заданное администратором).

TPE, получаемые майнером за обработку транзакции, используются для учета следующих затрат:

- Затраты на вычисления, выполняемые в рамках транзакции.
- Комиссия за количество данных, записываемых в РР.

Помимо учета затрат техническая комиссия работает как адаптивная защита от DoS атак мусорными транзакциями: атакующий (как и любой пользователь) должен тратить TPE для использования ресурса, включая вычисления, размер пересылаемых транзакций и хранение данных.

# 7. ПРОЕКТЫ ДЛЯ ПЛАТФОРМЫ

Далее приводятся описания проектов, которые предполагается размещать в сети **Мастерчейн** в краткосрочной перспективе.

## 7.1. ПРОЕКТ «ДЕЦЕНТРАЛИЗОВАННАЯ ДЕПОЗИТАРНАЯ СИСТЕМА ДЛЯ УЧЕТА ЗАКЛАДНЫХ»

### 7.1.1. ЦЕЛИ

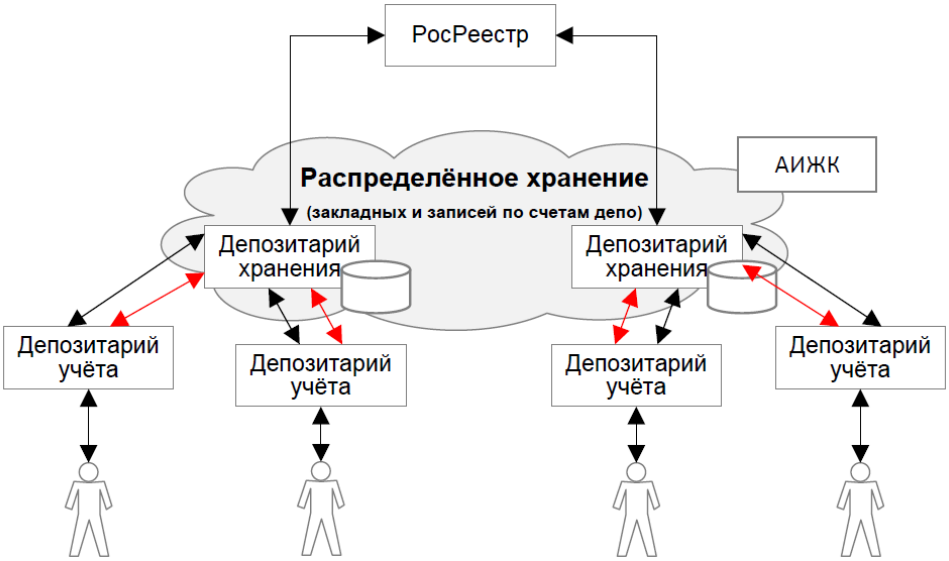
1. Вывести ДДС в эксплуатацию в соответствии со сроками вступления в силу требований об учете закладных в электронной форме.
2. Привлечь достаточное количество ипотечных банков для унификации решения на всем сегменте.
3. Обеспечить снижение стоимости и времени проведения операций по хранению, учету и секьюритизации закладных.

### 7.1.2. ЗАДАЧИ

1. Создать консорциум основных участников рынка по ипотечным закладным для участия в работе ДДС.
2. Разработать и реализовать решение ДДС как полностью Open Source «коробочное» решение.
3. Вывести ДДС в промышленное использование для учета электронных закладных к середине 2018 года.
4. Организовать Сервисную компанию (SPV) для обслуживания и упрощения договорных отношений между участниками ДДС.

### 7.1.3. ОПИСАНИЕ ПРОЕКТА

- Соответствует действующей правовой базе, сохраняется разделение ролей и функций существующих участников;
- Депозитарии хранения формируют «облако» для распределенного хранения электронных закладных и движений по депо-счетам;
- Процессы между участниками автоматизируются на смарт-контрактах, соответствующих логике действующего законодательства.




## 7.1.4. УЧАСТНИКИ ПРОЕКТА

- Банки, предоставляющие ипотечные кредиты, депозитарии;
- АИЖК;
- (опционально) Росреестр.

## 7.1.5. ПРОГНОЗ ЭКОНОМИЧЕСКОЙ ЧАСТИ

- Значительное (в 2-5 раз) снижение стоимости хранения, учета и подготовки/проведения секьюритизации.
- Снижение времени проведения операций с дней до минут.
- Надежность хранения закладных и операций по депо-счетам.
- После первого года эксплуатации, первая в мире система по количеству полностью электронных закладных (eMortgage).

# 7.2. ПРОЕКТ «KYC»

## 7.2.1. ЦЕЛИ

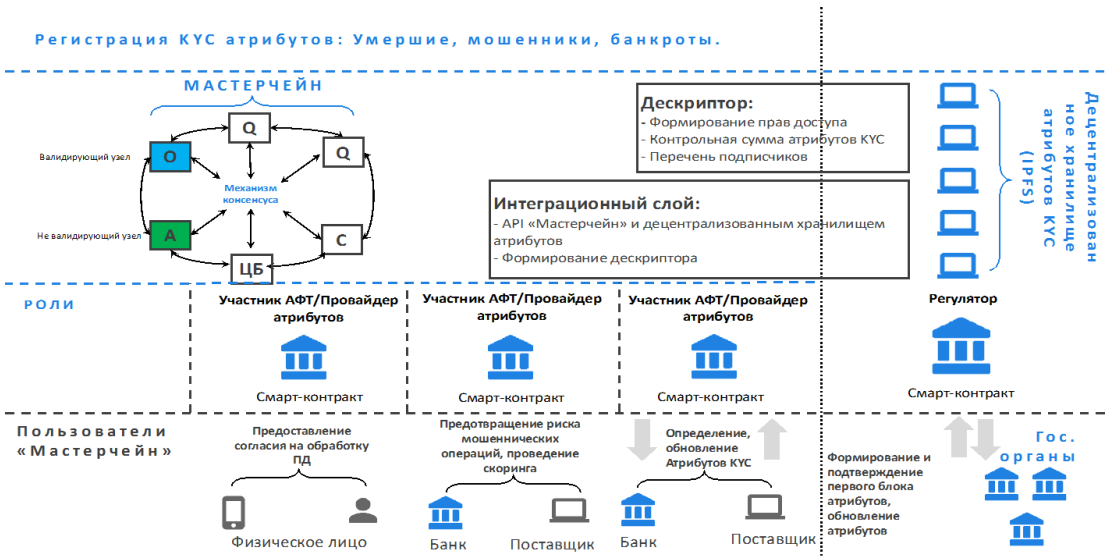
1. Обеспечение снижения риска отсутствия необходимой информации для предотвращения проведения мошеннических транзакций.
2. Обмен информацией о физических лицах (структура «KYC атрибуты») между участниками децентрализованной сети **Мастерчейн** без раскрытия сведений, составляющих банковскую тайну и персональные данные клиентов.
3. Обеспечение возможности масштабирования решения в части:
   - Возможности упрощенной идентификации – реализация концепция Digital Identity.
   - Обмена данными по юридическим лицам.
   - Обмена кредитными историями.

## 7.2.2. ЗАДАЧИ

1. Реализация бизнес-сценариев использования «концепции KYC».
2. Осуществление межбанковского взаимодействия без раскрытия клиентской базы на коммерческой основе.
3. Обеспечение исполнение №13-ФЗ (от 02.07.2017) в части соблюдения требований: по обезличиванию, уничтожению персональных данных, отсутствию игнорирования запросов от владельцев ПД.
4. Обеспечение контроля регулятором за процессом.

## 7.2.3. ОПИСАНИЕ ПРОЕКТА

Проект представляет собой имплементацию совместного доступа к децентрализованному хранилищу данных (структуры «KYC атрибуты») посредством технологии распределенных реестров на коммерческой основе.



Структура данных «KYC атрибуты» не хранится в децентрализованной сети Мастерчейн, а находится в обезличенном виде в децентрализованном хранилище (IPFS), интегрированном с децентрализованной сетью Мастерчейн.

Выполняемые операции в рамках проекта:

1. Осуществления доверительного обмена информацией по клиентам физическим лицам на коммерческой основе.
2. Сбор, обработка и формирование структуры данных «KYC атрибуты»:
   - Объективные атрибуты – не определяются поведенческим паттерном или взаимоотношениями, гарантированными государством.
   - Накапливаемые атрибуты – факты, которые могут изменяться в течение жизненного цикла физического или юридического лица.
   - Приобретенные атрибуты – данные, которые могут изменяться, являются идентификатором взаимоотношений с доверенным доменом данных.
3. Формирование децентрализованного хранилища, предоставление доступа согласно принятой концепции ролей и полномочий децентрализованной сети «Мастерчейн».
4. Осуществление бизнес-сценариев:
   - Проверка физических лиц на включение в реестр мошенников, выявленный участниками децентрализованной системы обмена сообщениями посредством проведения скоринга анкет физических лиц.
   - Проверка физических лиц на наличие факта о регистрации смерти.
5. Возможность масштабирования данного решения в будущем:
   - реализация процесса обмена кредитными историями клиентов (аналог БКИ);
   - реализация процесса обмена данными по юридическим лицам;
   - реализация процесса упрощенной/удаленной идентификации клиента;
   - расширение функционала системы для реализации полноценного KYC сценария.

## 7.2.4. УЧАСТНИКИ ПРОЕКТА

- Провайдер – участник децентрализованной сети, ответственный за сбор, обработку, передачу структуры данных «KYC атрибуты».
- Потребитель – участник децентрализованной сети, имеющий доступ и использующий данные «KYC атрибуты» для предотвращения проведения мошеннических операций.
- Физическое лицо – предоставляет/отзывает согласие на обработку ПД для формирования структуры данных «KYC атрибуты».
- Регулятор – осуществляет контроль/аудирование выбранного сценария\процесса на предмет соответствия, соблюдения законодательной базы, исполнения запросов физических лиц.

## 7.2.5. ПРОГНОЗ ЭКОНОМИЧЕСКОЙ ЧАСТИ

- Формирование доверительной среды для участников.
- Снижение риска проведения мошеннических операций.
- Обеспечение упрощенной/удаленной идентификации клиентов.

# 7.3. ПРОЕКТ «РАСПРЕДЕЛЕННЫЙ РЕЕСТР ЦИФРОВЫХ БАНКОВСКИХ ГАРАНТИЙ»

## 7.3.1. ЦЕЛИ

1. Снизить трудозатраты на процесс получения/проверки гарантии для всех участников цепочки: банк, принципал, бенефициар.
2. Повысить защищенность банковских гарантий и снизить количество подделок на бумаге.
3. Расширение возможностей банковских гарантий за счет использования смарт-контрактов.

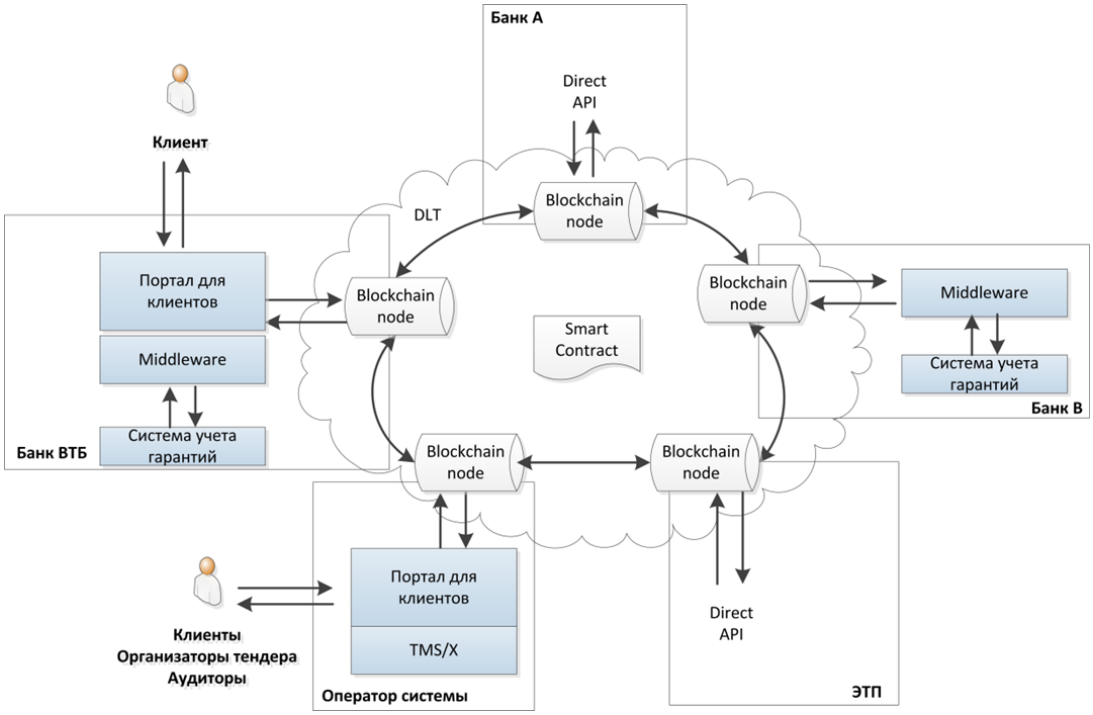
## 7.3.2. ЗАДАЧИ

1. Разработать и реализовать на базе **Мастерчейн** работающий прототип с Open API для подключения других участников.
2. Совместно с заинтересованными членами АФТ провести опытную эксплуатацию прототипа решения и (при необходимости) внести изменения в Open API (цель: минимизировать затраты на подключение внутренних систем Банков к системе).
3. Идентифицировать и разработать изменения (проекты) в законодательстве, необходимые для запуска в промышленную эксплуатацию.

## 7.3.3. ОПИСАНИЕ ПРОЕКТА

Финальной целью проекта является создание распределенного реестра цифровых банковских гарантий, выдаваемых банками, работающими на территории Российской Федерации, и уход от бумажных гарантий.

Предполагается, что цифровая гарантия будет первичным цифровым документом, который будет воспроизводиться на бумаге только при необходимости в целях информирования.



1. Система будет реализована на платформе Мастерчейн.
2. Непосредственные участники системы (банки) будут иметь свои узлы (nodes) в сети «Мастерчейн-гарантии» и клиентские порталы для предоставления информации клиентам.
3. ЭТП (как одни из основных потребителей информации о гарантиях) будут иметь специальный шлюз сопряжения с «Мастерчейн-гарантии» и специальные права.

## 7.3.4. УЧАСТНИКИ ПРОЕКТА

- Банки, действующие на территории РФ, имеющие право выдавать банковские гарантии. Выдача цифровых банковских гарантий и публикация информации о гарантии в реестре.
- Торговые площадки. Возможность получать из реестра информацию о гарантиях, имеющих отношение к сделкам на ТП.
- Представители юридических лиц. Возможность получать из реестра информацию о гарантиях, имеющих отношение к юридическому лицу.
- Физические лица. Возможность получать из реестра информацию о гарантиях, доступ к которым является публичным (например, гарантии в рамках 44-ФЗ).
- Представители органов государственной власти. Возможность получать из реестра информацию в рамках их полномочий и зон ответственности.

## 7.3.5. ПРОГНОЗ ЭКОНОМИЧЕСКОЙ ЧАСТИ

- Повышенная защищенность банковских гарантий.

  Цифровая гарантия, хранящаяся в доверенном распределенном цифровом реестре, сложнее подделывается, чем бумажный документ.
- Возможность расширить функционал гарантий, используя смарт-контракты.
- Снижение издержек и ускорение процесса выпуска банковских гарантий.

  Особенно важно для малого и среднего бизнеса, а также для банков, предоставляющих им гарантии. На большом количестве гарантий снижение издержек и эффект от ускорения будут больше.
- Расширение базы зарегистрированных банковских гарантий.

  В настоящее время существует централизованный реестр гарантий, выпущенных в связи с контрактами по 44-ФЗ – http://zakupki.gov.ru.
- Упрощение процесса проверки банковских гарантий третьими сторонами.
- Возможность разграничения прав доступа различных категорий пользователей системы как к банковским гарантиям, так и к отдельными разделам гарантии.

  В зависимости от категории пользователя системы регулируется как область видимости гарантий, так и область видимости внутри каждой гарантии. Например, спецусловия могут быть доступны только банку, принципалу, бенефициару и регулятору.

# 7.4. ЦИФРОВОЙ АККРЕДИТИВ

## 7.4.1. ЦЕЛИ

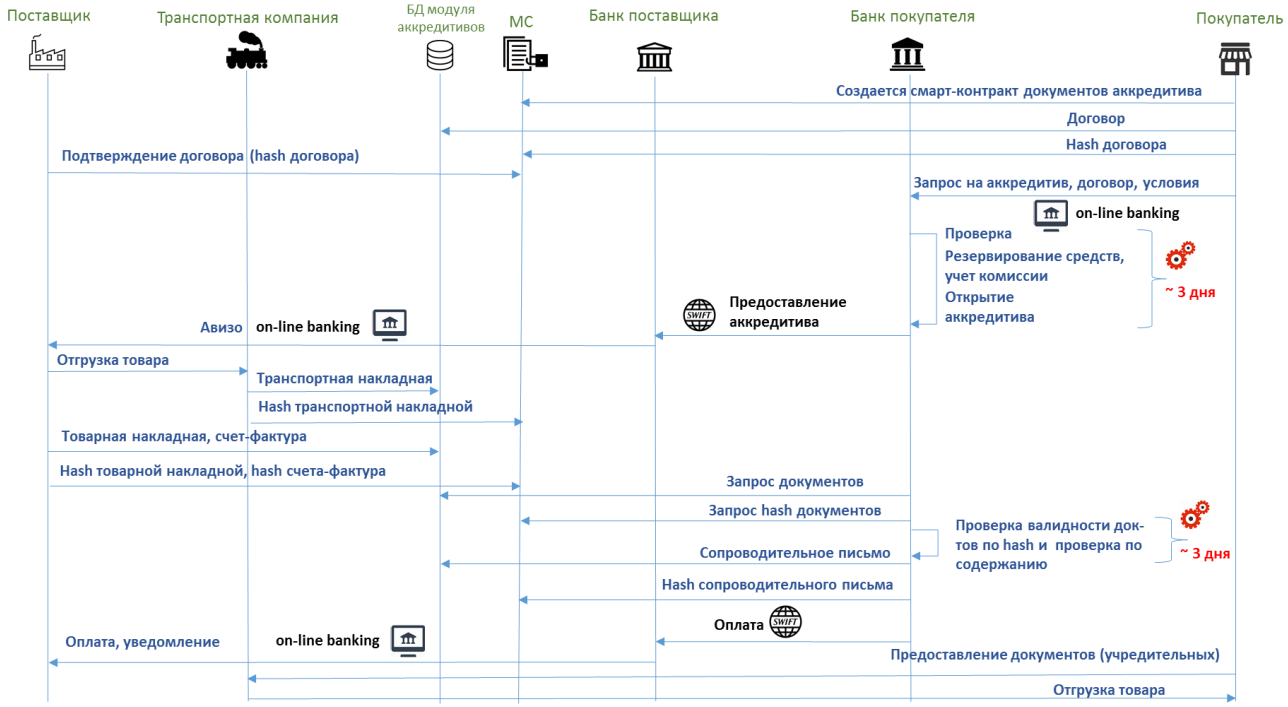
1. Сокращение сроков исполнения сделок по аккредитивам с покрытием.

## 7.4.2. ЗАДАЧИ

1. Исключить бумажный документооборот и связанные с ним задержки по времени при исполнении сделок (фаза 1).
2. Автоматизировать финансовые транзакции (фаза 2).

## 7.4.3. ОПИСАНИЕ ПРОЕКТА

Использование **Мастерчейн** в аккредитивных сделках с покрытием для устранения бумажного документооборота и сокращения сроков сделки.




## 7.4.4. УЧАСТНИКИ ПРОЕКТА

- Продавец;
- Банк, обслуживающий продавца;
- Покупатель;
- Банк, обслуживающий покупателя;
- Транспортная компания.

## 7.4.5. ПРОГНОЗ ЭКОНОМИЧЕСКОЙ ЧАСТИ

Сокращение срока реализации аккредитива с покрытием на 15 дней.

- Фаза 1: Сокращение на 9 дней.
- Фаза 2: Сокращение еще до 6 дней.


Ассоциация развития финансовых технологий
Москва, 2017