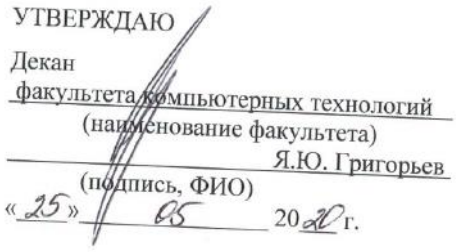
Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Комсомольский-на-Амуре государственный университет»




# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
# Обеспечение информационной безопасности в пиринговых сетях

| | |
|---|---|
| Направление подготовки | *10.05.03 "Информационная безопасность автоматизированных систем"* |
| Направленность (профиль) образовательной программы | *Обеспечение информационной безопасности распределенных информационных систем* |
| Квалификация выпускника | *специалист по защите информации* |
| Год начала подготовки *(по учебному плану)* | *2020* |
| Форма обучения | *очная* |
| Технология обучения | *традиционная* |

| Курс | Семестр | Трудоемкость, з.е. |
|---|---|---|
| *5* | *9* | *3* |

| Вид промежуточной аттестации | Обеспечивающее подразделение |
|---|---|
| *Зачет с оценкой* | *Кафедра ИБАС - Информационная безопасность автоматизированных систем* |

Комсомольск-на-Амуре 2020

Разработчик рабочей программы:

Доцент ИБАС к.э.н. _____ Власов А.А.

(должность, степень, ученое звание) (подпись) (ФИО)

СОГЛАСОВАНО:

Заведующий кафедрой

ИБАС _____ А.Ю.Лошманов

(наименование кафедры) (подпись) (ФИО)

## 1 Общие положения

Рабочая программа дисциплины «Обеспечение информационной безопасности в пиринговых сетях» составлена в соответствии с требованиями федерального государственного образовательного стандарта, утвержденного приказом Министерства образования и науки Российской Федерации № 1509 от 01.12.2016, и основной профессиональной образовательной программы подготовки «Анализ безопасности информационных систем»
по направлению 10.05.03 "Информационная безопасность автоматизированных систем".

Практическая подготовка реализуется на основе:
Профессиональный стандарт утвержденного приказом Министерства труда и социальной защиты от 15 сентября 2016 года N 522н №843 "Специалист по защите информации в автоматизированных системах" зарегистрированного в Министерстве юстиции Российской Федерации 28 сентября 2016 года, регистрационный N 43857.

| | |
|---|---|
| Задачи дисциплины | Раскрытие сущности и значения обеспечения информационной безопасности в пиринговых сетях, их места в системе национальной безопасности.<br>Определение теоретических, концептуальных, методологических, организационных и технических основ обеспечения безопасности информации в пиринговых сетях. |
| Основные разделы / темы дисциплины | **Раздел 1**<br>Тема 1 Терминология распределенных реестров<br>Тема 2 Исследование протоколов взаимодействия распределённых реестров<br>**Раздел 2**<br>Тема 3 Исследование функции обмена файлам и между одноранговыми устройствами<br>Тема 4 Исследование обмена файлами по сетям p2p |

## 2 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами образовательной программы

Процесс изучения дисциплины «Обеспечение информационной безопасности в пиринговых сетях» направлен на формирование следующих компетенций в соответствии с ФГОС ВО и основной образовательной программой (таблица 1):

Таблица 1 – Компетенции и планируемые результаты обучения по дисциплине

| Код и наименование компетенции | Планируемые результаты обучения по дисциплине | | |
|---|---|---|---|
| | Перечень знаний | Перечень умений | Перечень навыков |
| Профессиональные | | | |
| **ПК-23** способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа | **ПК-23.1** Знает способы формирования комплекса мер (правила, процедуры, методы) для | **ПК-23.2** Умеет выбрать комплекс мер (правила, процедуры, методы) для защиты информации | **ПК-23.3** Владеет навыками контроля мер (правил, процедуры методов) для защиты информации |

| | | | |
|---|---|---|---|
| | защиты информации ограниченного доступа | ограниченного доступа | ограниченного доступа |

## 3 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Обеспечение информационной безопасности в пиринговых сетях» изучается на 5 курсе(ах) в 9 семестре(ах).

Дисциплина входит в состав блока 1 «Дисциплины (модули)» и относится к базовой части.

Для освоения дисциплины необходимы знания, умения, навыки и (или) опыт практической деятельности, сформированные в процессе изучения дисциплин Организация и технология защиты конфиденциальной информации в информационных системах

Знания, умения и навыки, сформированные при изучении дисциплины «Обеспечение информационной безопасности в пиринговых сетях», будут востребованы при изучении последующих дисциплин: Подготовка к процедуре защиты и защита выпускной квалификационной работы.

Дисциплина «Обеспечение информационной безопасности в пиринговых сетях» частично реализуется в форме практической подготовки. Практическая подготовка организуется путем выполнения лабораторных работ.

Дисциплина «Обеспечение информационной безопасности в пиринговых сетях» в рамках воспитательной работы направлена на формирование у обучающихся умения аргументировать, самостоятельно мыслить, развивает профессиональные умения, ответственности за выполнение учебно-производственных заданий, проводить мониторинг защищенности информации в автоматизированных системах и оценку рисков информационной безопасности автоматизированных систем,

## 4 Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины составляет 3 з.е., 108 акад. час.

Распределение объема дисциплины (модуля) по видам учебных занятий представлено в таблице 2.

Таблица 2 – Объем дисциплины (модуля) по видам учебных занятий

| **Объем дисциплины** | **Всего академических часов** |
|---|---|
| Общая трудоемкость дисциплины | 108 |
| **Контактная аудиторная работа обучающихся с преподавателем (по видам учебных занятий), всего** | 64 |
| В том числе: | |
| **занятия лекционного типа** (лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации педагогическими работниками) | 32 |
| **занятия семинарского типа** (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия) | 32 |
| **Самостоятельная работа обучающихся и контактная работа**, включающая групповые консультации, индивидуальную работу | 44 |

| Объем дисциплины | Всего академических часов |
|---|---|
| обучающихся с преподавателями (в том числе индивидуальные консультации); взаимодействие в электронной информационно-образовательной среде вуза | |
| Промежуточная аттестация обучающихся – Зачет с оценкой | |

## 5 Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебной работы

Таблица 3 – Структура и содержание дисциплины (модуля)

| Наименование разделов, тем и содержание материала | Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах) | | | |
|---|---|---|---|---|
| | Контактная работа преподавателя с обучающимися | | | СРС |
| | Лекции | Семинарские (практические занятия) | Лабораторные занятия | |
| **Раздел 1**<br>Тема 1 Терминология распределенных реестров<br>Тема 2 Исследование протоколов взаимодействия распределённых реестров | 16 | | 16 | 22 |
| **Раздел 2**<br>Тема 3 Исследование функции обмена файлам имежду одноранговыми устройствами<br>Тема 4 Исследование обмена файлами по сетям p2p | 16 | | 16 | 22 |
| **ИТОГО по дисциплине** | **32** | | **32** | **44** |

## 6 Внеаудиторная самостоятельная работа обучающихся по дисциплине (модулю)

При планировании самостоятельной работы студенту рекомендуется руководствоваться следующим распределением часов на самостоятельную работу (таблица 4):

Таблица 4 – Рекомендуемое распределение часов на самостоятельную работу

| Компоненты самостоятельной работы | Количество часов |
|---|---|
| Изучение теоретических разделов дисциплины | 14 |
| Подготовка к занятиям семинарского типа | 15 |
| Подготовка и оформление РГР | 15 |
| | 44 |

## 7 Оценочные средства для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю)

Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации представлен в Приложении 1.

Полный комплект контрольных заданий или иных материалов, необходимых для оценивания результатов обучения по дисциплине (модулю), практике хранится на кафедре-разработчике в бумажном и электронном виде.

## 8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

### 8.1 Основная литература


1. Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов. - М.: ГЛТ, 2016. - 586 с.
2. Blockgeeks Inc, «Blockchain Glossary: From A-Z,» [В Интернете]. Available: https://blockgeeks.com/guides/blockchain-glossary-from-a-z.
3. BlockchainTechnologies.com Diversified Internet Holdings LLC, «Blockchain glossary,» [В Интернете]. Available: https://www.blockchaintechnologies.com/glossary/.
4. С. Базанов, «Криптовалюты: Термины и сокращения,» [В Интернете]. Available: https://medium.com/bitcoin-review/bitcoin-криптовалюты-термины-и-сокращения- 27293b8413cc.
5. Технический комитет по стандартизации Криптографическая защита информации, Термины и определения в области технологий цепной записи данных (блокчейн) и распределенных реестров. МР-26.4.001, Москва, 2018.
6. Федеральный закон «О цифровых финансовых активах», проект.


### 8.2 Дополнительная литература


1. SNatives] Implement mainline Ethereum precompiles. 2019. URL: https://github.com/hyperledger/burrow/ issues/1240 (дата обращения: 02.12.2019).
2. Brown, R. G. The Five Ingredients Of Blockchain Interoperability // Forbes, 2020. URL: https://www.forbes. com/sites/richardgendalbrown/2020/02/13/the-five-ingredients-of-blockchaininteroperability/#7d3e7ce558a1 (дата обращения 13.02.2020).
3. Buterin, V. Chain Interoperability. 2016. URL: https://www.r3.com/wp-content/uploads/2017/06/chain_ interoperability_r3.pdf (дата обращения: 14.11.2019).
4. Byzantine fault tolerance (BFT) and Crash fault tolerance (CFT) // Stack Overflow, 2019. URL: https:// stackoverflow.com/questions/56336229/byzantine-fault-tolerancebft-and-crash-fault-tolerance-cft (дата обращения: 11.11.2019).
5. Chainstack. Enterprise Blockchain Protocols: Evolution Index 2020. URL: https://chainstack.com/wp-content/ uploads/2020/01/Enterprise-Blockchain-Protocols-Evolution-Index-2020.pdf (дата обращения: 22.01.2020).
6. ECDSA: (v, r, s), what is v? // Stack Exchange, 2019. URL: https://bitcoin.stackexchange.com/ questions/38351/ecdsa-v-r-s-what-is-v (дата обращения: 09.12.2019).
7. Hash Time Locked Contracts // Bitcoin Wiki. URL: https://en.bitcoin.it/wiki/Hash_Time_Locked_Contracts (дата обращения: 04.12.2019).
8. Hyperledger Burrow. Hyperledger. 2019. URL: https://www.hyperledger.org/projects/hyperledger-burrow (дата обращения: 12.11.2019).
9. ISO/IEC 17788:2014 Information technology – Cloud computing – Overview and vocabulary. 2014. URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:17788:ed-1:v1:en (дата обращения: 10.12.2019).
10. Interledger Overview. Interledger. URL: https://interledger.org/overview.html (дата обращения: 10.12.2019). Internet of Value Manifesto. World Wide Web Consortium (W3C). URL: https://www.w3.org/Web-Commerce/
11. IG/wiki/Internet_of_Value_Manifesto (дата обращения: 12.12.2019). Lightning Network Documents. Lightning Network. URL: https://lightning.network/docs/ (дата обращения:

12. 03.12.2019).
Johnson S., Robinson P., Brainard J. Sidechains and interoperability. 2019. URL: https://arxiv.org/
13. abs/1903.04077 (дата обращения: 15.11.2019).
14. Tendermint. URL: https://docs.tendermint.com/ (дата обращения: 02.12.2019).
15. The Raft Consensus Algorithm. URL: https://raft.github.io/ (дата обращения: 03.12.2019).
16. Siris V., Nikander P., Voulgaris S., Fotiou N., Lagutin D., Polyzos G.C. Interledger Approaches. 2019. URL: https://ieeexplore.ieee.org/document/8755830 (дата обращения: 18.11.2019).
17. Zamyatin A., Al-Bassam M., Zindros D., Kokoris-Kogias E., Moreno-Sanchez P., Kiayias A., Knottenbelt W.J. SoK: Communication Across Distributed Ledgers. 2019. URL: https://eprint.iacr.org/2019/1128.pdf (дата обращения: 14.11.2019).

### 8.3 Методические указания для студентов по освоению дисциплины

Обучение дисциплине «Обеспечение информационной безопасности в пиринговых сетях», предполагает изучение курса на аудиторных занятиях и в ходе самостоятельной работы. Аудиторные занятия проводятся в форме лекций и практических занятий.

Таблица 5 Методические указания к отдельным видам деятельности

| Вид учебного занятия | Организация деятельности студента |
|---|---|
| Лекция | Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения. Выделять ключевые слова, формулы, отмечать на полях уточняющие вопросы по теме занятия |
| Лабораторные занятие | Работа с автоматизированными рабочими местами. |
| Самостоятельная работа | Для более глубокого изучения разделов дисциплины предусмотрены отдельные виды самостоятельной работы: подготовка к практическим занятиям, изучение теоретических разделов дисциплины, подготовка РГР. |

Самостоятельная работа является наиболее продуктивной формой образовательной и познавательной деятельности студента в период обучения. СРС направлена на углубление и закрепление знаний студента, развитие практических умений. СРС по дисциплине «Обеспечение информационной безопасности в пиринговых сетях» включает следующие виды работ:

– работу с лекционным материалом, поиск и обзор литературы и электронных источников информации по индивидуальному заданию;

– опережающую самостоятельную работу;

– изучение тем, вынесенных на самостоятельную проработку;

– подготовку к практическим занятиям;

– выполнение и оформление РГР.

Контроль самостоятельной работы студентов и качество освоения дисциплины осуществляется посредством:

– представления в указанные контрольные сроки результатов выполнения заданий для текущего контроля;

– выполнения и защиты РГР;

### 8.4 Современные профессиональные базы данных и информационные

**справочные системы, используемые при осуществлении образовательного процесса по дисциплине**

1. Электронно-библиотечная система ZNANIUM.COM – http://www. znanium.com.
2. Консультант+
3. Научная электронная библиотека Elibrary http://elibrary.ru.

### 8.5 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

1. Сайт университета www.knastu.ru[Электронный ресурс]:. Раздел сотрудникам, документы СМК, режим доступа – свободный. Загл. с экрана
2. Научная электронная библиотека Elibrary http://elibrary.ru.

С целью повышения качества ведения образовательной деятельности в университете создана электронная информационно-образовательная среда. Она подразумевает организацию взаимодействия между обучающимися и преподавателями через систему личных кабинетов студентов, расположенных на официальном сайте университета в информационно-телекоммуникационной сети «Интернет» по адресу https://student.knastu.ru. Созданная информационно-образовательная среда позволяет осуществлять взаимодействие между участниками образовательного процесса посредством организации дистанционного консультирования по вопросам выполнения практических заданий.

### 8.6 Лицензионное программное обеспечение, используемое при осуществлении образовательного процесса по дисциплине

Таблица 6 – Перечень используемого программного обеспечения

| Наименование ПО | Реквизиты |
|---|---|
| Microsoft® Windows Professional 7 Russian | Лицензионный сертификат № 46243844 от 09.12.2009 |
| Open Office или аналог | Свободно-распространяемое |
| Операционная система Kali Linux или аналог | Свободно-распространяемое |
| Операционная система Ubuntu или аналог | Свободно-распространяемое |
| Обозреватель Google Chrome или аналог | Свободно-распространяемое |

## 9 Организационно-педагогические условия

Организация образовательного процесса регламентируется учебным планом и расписанием учебных занятий. Язык обучения (преподавания) — русский. Для всех видов аудиторных занятий академический час устанавливается продолжительностью 45 минут.

При формировании своей индивидуальной образовательной траектории обучающийся имеет право на перезачет соответствующих дисциплин и профессиональных модулей, освоенных в процессе предшествующего обучения, который освобождает обучающегося от необходимости их повторного освоения.

### 9.1 Образовательные технологии

Учебный процесс при преподавании курса основывается на использовании традиционных, инновационных и информационных образовательных технологий.

Традиционные образовательные технологии представлены лекциями и семинарскими (практическими) занятиями. Инновационные образовательные технологии используются в виде широкого применения активных и интерактивных форм проведения занятий. Информационные образовательные технологии реализуются путем активизации самостоятельной работы студентов в информационной образовательной среде.

**9.2 Занятия лекционного типа**

Лекционный курс предполагает систематизированное изложение основных вопросов учебного плана.

На первой лекции лектор обязан предупредить студентов, применительно к какому базовому учебнику (учебникам, учебным пособиям) будет прочитан курс.

Лекционный курс должен давать наибольший объем информации и обеспечивать более глубокое понимание учебных вопросов при значительно меньшей затрате времени, чем это требуется большинству студентов на самостоятельное изучение материала.

**9.3 Занятия семинарского типа**

Семинарские занятия представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы.

Основной формой проведения семинаров является обсуждение наиболее проблемных и сложных вопросов по отдельным темам, а также разбор примеров и ситуаций в аудиторных условиях. В обязанности преподавателя входят: оказание методической помощи и консультирование студентов по соответствующим темам курса.

Активность на семинарских занятиях оценивается по следующим критериям:

· ответы на вопросы, предлагаемые преподавателем;

· участие в дискуссиях;

· выполнение проектных и иных заданий;

· ассистирование преподавателю в проведении занятий.

Ответ должен быть аргументированным, развернутым, не односложным, содержать ссылки на источники.

Доклады и оппонирование докладов проверяют степень владения теоретическим материалом, а также корректность и строгость рассуждений.

Оценивание заданий, выполненных на семинарском занятии, входит в накопленную оценку.

**9.4 Самостоятельная работа обучающихся по дисциплине (модулю)**

Самостоятельная работа студентов – это процесс активного, целенаправленного приобретения студентом новых знаний, умений без непосредственного участия преподавателя, характеризующийся предметной направленностью, эффективным контролем и оценкой результатов деятельности обучающегося.

Цели самостоятельной работы:

· систематизация и закрепление полученных теоретических знаний и практических умений студентов;

· углубление и расширение теоретических знаний;

· формирование умений использовать нормативную и справочную документацию, специальную литературу;

· развитие познавательных способностей, активности студентов, ответственности и организованности;

· формирование самостоятельности мышления, творческой инициативы, способностей к саморазвитию, самосовершенствованию и самореализации;

· развитие исследовательских умений и академических навыков.

Самостоятельная работа может осуществляться индивидуально или группами студентов в зависимости от цели, объема, уровня сложности, конкретной тематики.

Технология организации самостоятельной работы студентов включает использование информационных и материально-технических ресурсов университета.

Контроль результатов внеаудиторной самостоятельной работы студентов может проходить в письменной, устной или смешанной форме.

Студенты должны подходить к самостоятельной работе как к наиважнейшему средству закрепления и развития теоретических знаний, выработке единства взглядов на отдельные вопросы курса, приобретения определенных навыков и использования профессиональной литературы.

### 9.5 Методические указания для обучающихся по освоению дисциплины

При изучении дисциплины обучающимся целесообразно выполнять следующие рекомендации:

1. Изучение учебной дисциплины должно вестись систематически.
2. После изучения какого-либо раздела по учебнику или конспектным материалам рекомендуется по памяти воспроизвести основные термины, определения, понятия раздела.
3. Особое внимание следует уделить выполнению отчетов по практическим занятиям и индивидуальным комплексным заданиям на самостоятельную работу.
4. Вся тематика вопросов, изучаемых самостоятельно, задается на лекциях преподавателем. Им же даются источники (в первую очередь вновь изданные в периодической научной литературе) для более детального понимания вопросов, озвученных на лекции.

При самостоятельной проработке курса обучающиеся должны:

· просматривать основные определения и факты;

· повторить законспектированный на лекционном занятии материал и дополнить его с учетом рекомендованной по данной теме литературы;

· изучить рекомендованную литературу, составлять тезисы, аннотации и конспекты наиболее важных моментов;

· самостоятельно выполнять задания, аналогичные предлагаемым на занятиях;

· использовать для самопроверки материалы фонда оценочных средств.

**1. Методические указания при работе над конспектом лекции**

В ходе лекционных занятий необходимо вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации, положительный опыт в ораторском искусстве. Желательно оставить в рабочих конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

**2. Методические указания по самостоятельной работе над изучаемым материалом и при подготовке к лабораторным занятиям**

Начинать надо с изучения рекомендованной литературы. Необходимо помнить, что на лекции обычно рассматривается не весь материал, а только его часть. Остальная его часть восполняется в процессе самостоятельной работы. В связи с этим работа с рекомендованной литературой обязательна. Особое внимание при этом необходимо обратить на содержание основных положений и выводов, объяснение явлений и фактов, уяснение практического приложения рассматриваемых теоретических вопросов. В процессе этой работы необходимо стремиться понять и запомнить основные положения рассматриваемого материала, примеры, поясняющие его, а также разобраться в иллюстративном материале. Оформлять отчеты следует руководствуясь внутренними нормативными документами КнАГУ.

**3. Методические указания для выполнения лабораторных работ и РГР**

**Лабораторная работа 1**

**Терминология распределенных реестров**

***Задачи***

***Часть 1. Формирование понятийного аппарата.***

***Часть 2. Исследование теоретических аспектов цифровых финансовых активов.***

# Базовые термины

| | |
|---|---|
| 51% Attack / Атака 51% | 1) Ситуация, в которой более половины вычислительных мощностей всей децентрализованной сети контролируется одним лицом или группой лиц. Это лицо или группа лиц могут публиковать конфликтующие операции и навредить сети, если уних есть намерения этой сделать [1]<br>2) Атака на блокчейн, которая заключается в завладении группой майнеров более 50% вычислительных мощностей. Обычно используется применительно к Биткоину. [2]<br>3) Состояние, когда более половины вычислительной мощности сети криптовалюты контролируется одним майнером или группой майнеров. Теоретически, этот объём вычислительной мощности дает власть над сетью. Это означает, что каждая клиентская программа в сети верит в подтвержденный блок транзакций атакующей стороны. Это дает им контроль над сетью, включая следующие полномочия:<br>a) создавать транзакции, конфликтующие с чужими;<br>b) останавливать подтверждение чьей-либо транзакции;<br>c) тратить одни и те же монеты несколько раз;<br>d) мешать другим майнерам создавать действительные блоки.[3]<br><br>ЦТРР) Состояние, при котором более половины вычислительной мощности сети распределенного реестра контролируется группой аффилированных участников. В зависимости от алгоритма консенсуса реестра это может приводить к различнымнежелательным последствиям. |
| Block / Блок | 1) Пакеты, в которых в неизменном виде хранятся данные на блокчейне. [1]<br>2) Список проверенных транзакций, который добавляется к блокчейну в результате майнинга. Является базовым элементом структуры блокчейна. Состоит из двух частей—заголовка(Head) и полезной нагрузки (Payload) - собственно записи транзакций. [2] |

| | |
|---|---|
| | атаку, направленную на повторное использование электронных монет. [2]<br><br>ЦТРР) Зарегистрированный распределенным реестром факт взаимодействия |
| Consensus / Консенсус | 1) Консенсус достигается тогда, когда все участники сети согласны относительно валидности транзакций и все реестры – точная копия друг друга. [1]<br><br>ЦТРР) Алгоритм взаимодействия узлов распределенного реестрадля принятия решений по изменению и синхронизации информации |
| Cryptocurrency / Криптовалюта | 1) Криптовалюты (также известные как токены) – это представление цифровых активов. [1]<br>2) Форма цифровой валюты, основанная на математических методах, где посредством криптографических протоколов регулируется генерация единиц валюты и верификация переводов. Системы криптовалют функционируют независимо от центрального банка. [2]<br>3) Распределенная и децентрализованная система безопасного обмена и передачи цифровых денежных знаков, основанной на средствах криптографии. [3]<br>4) Биткоин, иной цифровой знак (токен), используемый в международном обороте в качестве универсального средства обмена (Беларусь) [4]<br>5) Виртуальная валюта, которая используется для платежей и транзакций, которые проходят через децентрализованную систему участников. (МВФ)<br>6) Вид цифрового финансового актива, создаваемый и учитываемый в распределенном реестре цифровых транзакций участниками этого реестра в соответствии с правилами ведения реестра цифровых транзакций. [7]<br><br>ЦТРР) Совокупность публичного распределенного реестра использующего единый формат монет и возможности сбыта и обмена этих монет на другие товары и услуги. |
| Cryptographic Hash Function / Криптографическая хэш-функция | 1) Криптографическая хэш-функция генерирует уникальный хэш заданной длины на основе нефиксированных по объему данных об операции. [1]<br><br>ЦТРР) Функция отображающая массивы информации не детерминированного размера в битовую строку заданного размера, обладающая криптографическим описанием свойств и характеристик |
| Decentralization / Децентрализация | 1) Передача полномочий на принятие решений и ответственности от централизованной организации, правительства или иного института к децентрализованной сети [2]<br><br>ЦТРР) Распределение процессов, происходящих в рамках единого центра принятия решений, на набор независимых исполнителей |
| Decentralized Application (DApp) / | 1) Приложение с открытым кодом, доверие к которому основано на доверии к коду, который исполняется на децентрализованной |

| | |
|---|---|
| Децентрализованное приложение | сети, а не на централизованном сервере. [2]<br><br>ЦТРР) Приложение, исполняемое и хранящееся в распределенной вычислительной среде, например поверх распределенного реестра |
| Digital Identity / Цифровая идентичность | 1) Идентичность, принадлежащая личности, организации или электронном устройству в электронном пространстве. [2]<br><br>ЦТРР) Совокупность средств хранения, протокола передачи, и мер защиты информации однозначно характеризующих сущности |
| Digital Signature / Цифровая подпись (ЭЦП—электронная цифровая подпись) | 1) Цифровой код, сгенерированный с использованием публичного ключа и присоединенный к документу в электронной форме, чтобы подтвердить неизменность его содержания и подтвердить личность отправителя. [1] |
| Distributed Ledger / распределенный реестр | 1) Реестр, где данные хранятся в сети децентрализованных узлов. Децентрализованный реестр не обязательно имеет собственную валюту, может быть частным, либо новые участники для присоединения к нему должны иметь специальное разрешение. [1]<br>2) Тип базы данных, которая распределена между разными географическими точками, странами, организациями. Все записи хранятся в едином реестре записей. [2]<br>3) Технология распределенного реестра учета — комбинация компонентов, включающих в себя сети peer-to-peer (P2P), распределенное хранение данных и криптографию. [3]<br>4) тип базы данных или системы записей, которая совместно используется, реплицируется и синхронизируется между членами сети. Распределенный реестр записывает синхронно и многоместно проводки, такие как обмен данными между участниками сети, что исключает возможность изменения любой отдельной копии записи в реестре (ЦСР)<br><br>ЦТРР) Инструмент построения распределенной сети хранения информации, предоставляющий ряд гарантий в условиях взаимного недоверия участников. Узлы сети распределенного реестра могут находиться в независимых, конкурирующих средах, поддерживая единое состояние хранимых данных. Гарантии, возможности и правила работы определяются алгоритмом принятия консенсусных решений используемым конкретным реестром. |
| Double Spending / Двойная трата или двойное расходование | 1) Случай, когда одна и та же сумма денег расходуется дважды. [1]<br>2) Ситуация в сети Блокчейн, когда кто-то пытается отправитьодин биткоин двум получателям одновременно. Однако когда транзакция подтверждена, отправить те же самые биткоины уже другому получателю невозможно. Чем больше подтверждений есть у каждой отдельной операции, тем сложнее организовать двойное расходование. [2]<br>3) Попытка потратить деньги дважды. Это происходит, когда кто-то выполняет финансовую транзакцию, а затем совершает вторую сделку с теми же самыми деньгами. [3]<br><br>ЦТРР). Повторное использование пользователем уже потраченного обеспечения транзакций, принятого в распределенном реестре |

| | |
|---|---|
| Exchange / Биржа | 1) Площадка, функционирующая как место торговли, соединяя покупателей и продавцов виртуальных валют, предоставляя платформу, на которой они могут предлагать и запрашиватьцены покупки/продажи. В отличие от операторов обмена криптовалют, платформы непосредственно не вовлечены в покупку/продажу (ЕЦБ)<br>2) Место для покупки и продажи криптовалюты. В большинстве случаев биржа взимает комиссии за операции обмена, выводу денежных средств. |
| Fiat / Фиат | Фиатные деньги—деньги, выпускаемые государством. [3] |
| Fork / Форк | 1) Форк создает альтернативную версию блокчейна, в результате чего на разных участках сети одновременно существуют два отдельных блокчейна. Форк может быть намеренным или случайным [1]<br>2) Создание альтернативной успешной версии цепочки блоков. Это может происходить умышленно, когда группа майнеров получает слишком много контроля над сетью (см. атаку 51%), случайно (одновременная запись новых блоков разными майнерами или из-за ошибки в системе), или целенаправленно, когда команда разработчиков решает представить новые функции в новой версии клиентской программы. Форк успешен, если он становится самой длинной версией цепочки блоков с точки зрения сложности. В этом случае альтернативная ветка блокчейна отвергается и становится невалидной. Также форком называют изменение программного протокола криптовалюты, которое создает две отдельные версии блокчейна с общей историей. Часто форком называют новую криптовалюту, которая построена на протоколе существующей. Например, лайткоин (LTC) является форком биткоина (BTC). [3] |
| Genesis Block / Начальный блок | 1) Первый или несколько первых блоков на блокчейне. [1]<br>2) Блок, добавленный в блокчейн при первичном внесении данных. [5] |
| ICO (Initial Coin Offering) / первоначальное предложение монет | Способ привлечения первичного капитала с использованием криптовалюты. [3] |
| Keys / Ключи | Строка символов (битовая строка), используемаякриптографическим алгоритмом при шифровании и дешифровании сообщений, постановке и проверке цифровой подписи, а также идентификации. Ключи бывают симметричные (один и тот же ключ используется для шифрования и дешифрования) и<br>ассиметричные (публичный и приватный). [3] |
| Mining / Майнинг | 1) Деятельность по валидации транзакций на блокчейне. Поскольку валидация транзакций является важным элементом работы блокчейна, манеры получают за него вознаграждение, обычно в форме монет. [1]<br>2) Необходимый и важный процесс в сети Биткоина и других криптовалют, в результате которого в блокчейн добавляется новый блок транзакций и происходит эмиссия монет. [3]<br>3) Отличная от создания собственных цифровых знаков деятельность, направленная на обеспечение функционирования |

| | |
|---|---|
| | реестра блоков транзакций посредством создания в таком реестре новых блоков с информацией о совершенных операциях. Лицо, осуществляющее майнинг, становится владельцем цифровых знаков, возникших в результате его деятельности по майнингу, и может получать цифровые знаки в качестве вознаграждения за верификацию совершения операцийв реестре блоков транзакций (Беларусь) [4]<br>4) Предпринимательская деятельность, направленная на создание криптовалюты и/или валидацию с целью получения вознаграждения в виде криптовалюты. [7] |
| Pool, mining pool / Пул, Майнинг-пул | Собрание майнеров, которые коллективно добывают блок, а затем делят полученное вознаграждение. Майнинг-пулы—способ увеличить доходность при росте сложности майнинга. [3] |
| Multi-Signature / Мультиподпись | Использование мультиподписи обеспечивает дополнительный уровень защиты: для авторизации транзакции необходим не один ключ, а несколько. [1] |
| Obfuscation / Обфускация | (Запутывание, сбивание с толку)—технология, позволяющая увеличить степень анонимности криптовалютных транзакций. [3] |
| Oracles / Оракулы | Мост между реальным миром и блокчейном, они являются источником данных для функционирования смарт-контрактов. [1] |
| Одноранговая сеть узлов, сеть p2p (peerto peer) | 5) Децентрализованное взаимодействие между двумя и более сторонами в сети, где все участники связаны со всеми. Участники P2P сети взаимодействуют напрямую между собой, минуя центрального контрагента [1]<br>6) Одноранговая компьютерная сеть, в которой все участники (узлы) равноправны и могут взаимодействовать друг с другом, являясь клиентом и сервером одновременно. [3]<br>7) Совокупность равнозначных для сети цифровых устройств и алгоритмов (протоколов) обмена данными между ними непосредственно, без посредников, без центрального (приоритетного) звена и возможности контроля со стороны (автоматически). |
| Public Address / Публичный адрес | Криптографический хэш открытого ключа. Они, как, например, и адреса электронной почты, могут быть опубликованы в открытом доступе (в отличие от закрытых ключей). [1] |
| Smart Contracts / Умные контракты (смарт-контракты) | 1) Смарт-контракты формализуют бизнес-правила в виде программного кода, который запускается на блокчейне и принимается всеми участниками сети. [1]<br>2) Механизм, включающий цифровые активы и две или более стороны, которые вкладывают активы в контракт, после чего они автоматически распределяются между этими сторонами, согласно формуле, основанной на показателях, значения которых неизвестны на момент подписания контракта. [3]<br>3) Умный контракт (smart-contract), чейнкод (chaincode): совокупность условий и последовательность действий, описанные в соответствии с политиками и процедурами ИС. Выполнение всех оговоренных условий, зависящее от конкретного состояния (состояний) ИС (в том числе, в результате проверки внешних по отношению к ИС условий), влечет автоматическое выполнение заранее определенной последовательности действий. Выполнение указанной последовательности действий, в свою очередь, также ведет к |

| | |
|---|---|
| | изменению состояния ИС. [5]<br>4) Программный код, предназначенный для функционирования в реестре блоков транзакций (блокчейне), иной распределенной информационной системе в целях автоматизированного совершения и (или) исполнения сделок либо совершения иных юридически значимых действий (Беларусь) [4]<br>5) Управляемая на основе событий программа, которая работает на распределенной, децентрализованной, коллективной и воспроизводимой системе регистрации записей и которая может удерживать и переводить активы (Аризона) [4]<br>6) Договор в электронной форме, исполнение прав и обязательств по которому осуществляется путем совершения в автоматическом порядке цифровых транзакций в распределенном реестре цифровых транзакций в строго определенной им последовательности и при наступлении определенных им обстоятельств. Защита прав участников (сторон) смарт-контракта осуществляется в порядке, аналогичном порядку осуществления защиты прав сторон договора, заключенного в электронной форме. [7] |
| State channels / Каналы состояния | 1) Технология, позволяющая проводить обмен информацией (транзакциями) между узлами в сети без предварительной записи в блокчейн. Идея каналов состояния заключается в перемещении многих промежуточных процессов вне блокчейна,сохранив при этом характерную надежность блокчейна. [3]<br>2) Обособленный канал ИС с реестром: способ взаимодействия между участниками ИС с реестром, обеспечивающий изоляцию данных (транзакции, блоки) от других участников в соответствии с конфигурацией ИС. [5] |
| Token / Токен | 1) Цифровой актив, выпускаемый с целью привлечения инвестиций в криптовалютный проект или компанию. Разновидность криптовалюты, но по своим свойствам ближе к акции или облигации. Выпускаются в ходе ICO и затемторгуются на криптовалютных биржах наравне с криптовалютами. [3]<br>2) Запись в реестре блоков транзакций, иной распределенной информационной системе, которая удостоверяет наличие у владельца цифрового знака (токена) прав на объекты гражданских прав и (или) является криптовалютой (Беларусь) [4]<br>3) Вид цифрового финансового актива, который выпускается юридическим лицом или индивидуальным предпринимателем (далее – эмитент) с целью привлечения финансирования и учитывается в реестре цифровых записей. [7] |
| Transaction / Транзакция | 1) Перевод денег между двумя адресами. [3]<br>2) Наименьший элемент взаимодействия, который представляет собой обмен информацией между двумя или более пользователями и/или ИС. [на основе ГОСТ Р 55681-2013 / ISO/TR 26122:2008 (пункт 3.5)] Транзакции могут быть как записаны, так и не записаны в реестр. Транзакцию, не записанную в реестр, будем называть неподтвержденной, а записанную – подтвержденной. [5] |
| Transaction Block / | 3) Группа транзакций, собранная в одну группу и которая может |

| | |
|---|---|
| Блок транзакций | хэширована и добавлена к блокчейну. [1]<br>4) Данные, содержащие набор из одной или нескольких снабжённых отметками времени транзакций и, возможно, дополнительную информацию. [на основе определения, предложенного ISO TC 307/SG1] [5] |
| Transaction Fee / Комиссия за проведение транзакции | Все транзакции с криптовалютой требуют выплаты небольшой комиссии. Эта комиссия добавляется к награде майнера за обработку блоков. [1] |
| Digital wallet / Цифровой кошелек | 1) Файл, в котором хранятся секретные ключи. Обычно включает в себя специальное программное обеспечение, которое позволяет просматривать и инициировать транзакции на томблокчейне, для которого этот кошелек создан. [1]<br>2) Программное приложение, позволяющее производить транзакцию с заданного адреса и просматривать его баланс. [3]<br>3) Программно-техническое средство, позволяющее хранить информацию о цифровых записях и обеспечивающее доступ к реестру цифровых транзакций. [6] |
| Zero Knowledge Proof / Доказательство с нулевым разглашением | Интерактивный криптографический протокол, позволяющий однойиз взаимодействующих сторон («The verifier»—Проверяющей) убедиться в достоверности какого-либо утверждения (обычно математического), не имея при этом никакой другой информации от второй стороны («The prover»—Доказывающей). [3] |
| Цифровой финансовый актив | Имущество в электронной форме, созданное с использованием шифровальных (криптографических) средств. Права собственности на данное имущество удостоверяются путем внесения цифровых записей в реестр цифровых транзакций. К цифровым финансовым активам относятся криптовалюта, токен. Цифровые финансовые активы не являются законным средством платежа на территории Российской Федерации. [6] |
| Цифровая транзакция | Действие или последовательность действий, направленных на создание, выпуск, обращение цифровых финансовых активов. [6] |
| Цифровая запись | Информация о цифровых финансовых активах, зафиксированная в реестре цифровых транзакций. [6] |
| Реестр цифровых транзакций | Формируемая на определенный момент времени систематизированная база цифровых записей. [6] |
| Участники реестра цифровых транзакций | Лица, осуществляющие цифровые транзакции в соответствии с правилами ведения реестра цифровых транзакций. [6] |
| Валидатор | Юридическое или физическое лицо, являющееся участником реестра цифровых транзакций и осуществляющее деятельность по валидации цифровых записей в реестре цифровых транзакций всоответствии с правилами ведения реестра цифровых транзакций. [6] |
| Валидация цифровой записи | Юридически значимое действие по подтверждению действительности цифровых записей в реестре цифровых транзакций, осуществляемое в порядке, установленном правилами ведения реестра цифровых транзакций. [6] |
| **Специальные термины, названия** | |
| Bitcoin | 1) Децентрализованная криптовалюта на открытом коде, которая оборачивается на глобальной P2P сети, без центрального контрагента или посредника. [1] |

| | |
|---|---|
| | 2) Одноранговая цифровая денежная система, построенная на криптографических алгоритмах. Расчетная единица в этой системе называется биткоин (bitcoin),—пишется со строчной буквы в отличие от названия денежной системы, которое пишется с прописной буквы. Биткоин—первая массовая криптовалюта. [3] |
| CryptoNote | Протокол, обеспечивающий обфускацию (запутывание) транзакций с целью увеличения степени анонимности. [3] |
| ECDSA (Elliptic Curve Digital Signature Algorithm) | Алгоритм, используемый для подтверждения транзакций в протоколе Bitcoin. [3] |
| Equihash | Алгоритм хэширования, применяемый в Proof-of-Work некоторых криптовалют (ZCash, Bitcoin Gold и др.). Представляет собой довольно сложную функцию хэширования и требует много оперативной памяти для выполнения. Оптимизирован для майнинга при помощи графических карт, т.н. GPU-майнинга. [3] |
| ERC20 Token Standard | Технический стандарт для смарт-контрактов, которому должны соответствовать токены в Ethereum. Фактически представляетсобой перечень требований, соблюдение которых обеспечивает нормальную работу токена в сети Ethereum. [2] |
| ERC721 Token Standard | Стандарт для неконвертируемых токенов в сети Ethereum. Неконвертируемый – означает цифровой актив, который не подлежит обмену. [2] |
| ERC223 Token Standard | Стандарт для токенов, с акцентом на безопасности, который позволяет пересылать токены так же, как и ETH, чтобы избежать потери токенов. Этот стандарт – улучшенная версия стандарта ERC20. [2] |
| Ether ETH | Интегральный элемент (т.е. специфичная валюта) в сети Ethereum. Ether поддерживает функционирование экосистемы Ethereum. Он является как форма стимулирования или форма поощрения, в целях исполнения операций в сети. [2] |
| Ethereum | 1) Платформа, основанная на открытом коде, где разработчики создают и запускают децентрализованные приложения, которые повышают ценность экосистемы Ethereum. Ethereum – это открытая децентрализованная сеть. [2]<br>2) Ethereum – это основанная на блокчейне децентрализованная платформа для запуска смарт-контрактов. Используется для решения проблем, связанных с цензурой, мошенничеством и вмешательством третьих сторон. [1] |
| EVM (Ethereum Virtual Machine) | Полная по Тьюрингу виртуальная машина, которая позволяет запускать байт-код EVM. Каждый узел в Ethereum работает на виртуальной машине, чтобы обеспечить консенсус на блокчейне. [1] |
| Lightning Network (LN) | Технологическое решение по масштабированию биткоина и других криптовалют (Lightcoin etc.). Предложено компанией Blockstream. Представляет собой надстройку над протоколом биткоина, которая позволяет проводить транзакции без предварительной записи в блокчейн. Функционирует в виде двунаправленных платежных каналов. [3] |
| MAST (Merkelized Abstract Syntax Trees) / | Технология расширения Биткоина, которая позволяет повысить гибкость смарт-контрактов, улучшить масштабируемость, и увеличить приватность. Объединяет потенциал P2SH с |

| | |
|---|---|
| Меркелизованные абстрактные синтаксические деревья | возможностями деревьев Меркла. Находится в стадии разработки. [3] |
| Solidity | 1) Язык программирования в Ethereum, который используется для разработки смарт-контрактов. [1]<br>2) Язык программирования на платформе Ethereum для разработки умных контрактов. [3] |
| SPV (Simplified Payment Verification) / Упрощенная верификация платежей | Особенность протокола Bitcoin, которая позволяет нодам заверять транзакцию без загрузки полной цепочки блоков. Вместо этого для верификации транзакции достаточно загрузки заголовков (Head) блоков, в которых содержатся хэши. [3] |
| **Алгоритмы консенсуса** | |
| Proof of Work / Процедура приходак консенсусу с доказательством работы | 1) Алгоритм достижения консенсуса, который требует активной работы по майнингу блоков, обычно требующей ресурсов, например, электроэнергии. Чем больше делается «работы» или чем больше выделяется вычислительных ресурсов, тем большую награду получает участник. [1]<br>2) Алгоритм, при помощи которого сеть майнинга биткоина приходит к консенсусу, определяя какой из майнинговых узлов запишет сформированный блок в блокчейн. Суть PoW сводится к двум основным пунктам:<br>a) Необходимости выполнения определенной достаточно сложной и длительной вычислительной задачи.<br>b) Возможности быстро и легко проверить результат. [3]<br>3) Процедура консенсуса на основе решения некоторой задачи с заданным уровнем вычислительной сложности, при этом, корректность полученного ответа может быть подтверждена валидатором. Как правило, проверка корректности решения является эффективно разрешимой задачей. [5]<br>4) Алгоритм консенсуса в DLT, в котором право удостоверения блока дается участнику на основании выполнения им некоторой достаточно сложной работы, которая удовлетворяет заранее определенным критериям. |
| Proof of Stake / Процедура приходак консенсусу с доказательством доли | 1) Алгоритм достижения консенсуса, в котором размер вознаграждения зависит от того, сколько у участника уже есть монет. Чем больше участник инвестирует в монеты, тем больше получает посредством майнинга. [1]<br>2) Альтернативный PoW алгоритм достижения консенсуса при записи блока в блокчейн, при котором вероятность записи нового блока в блокчейн и получение соответствующего вознаграждения пропорциональна доле владения пользователя в системе: отдельно взятый держатель валюты, имеющий долю P от общего числа монет в обороте, создает новый блок с вероятностью P. [3]<br>3) Процедура консенсуса на основе оценки числа условных единиц ИС, соотнесенных в определенный момент времени с пользователем. [5] |
| Proof-of-authority (PoA) / Процедура | Процедура консенсуса на основе разграничения прав пользователей. [5] |

| | |
|---|---|
| прихода к онсенсусу с доказательством права | |
| Delegated Proof-of-Stake (DPoS) | Алгоритм достижения консенсуса в децентрализованой среде, альтернативный консенсусам PoW и PoS. Был разработан в 2014 году в рамках проекта Graphene и впервые был задействован в проекте Bitshares, позже в проекте Steemit. [3] |
| PoI (Proof-of-Importance) | Альтернативный PoW алгоритм достижения консенсуса при записи блока в блокчейн, при котором определение пользователя, который будет записывать следующий блок, происходит с учетом вклада каждого участника процесса в развитие и продвижение криптовалюты. [3] |
| Hybrid PoS/PoW / Гибридный PoS/PoW | Гибридный алгоритм достижения консенсуса PoS/PoW позволяет одновременно использовать и Proof of Stake, и Proof of Work процедуры для достижения консенсуса. В этом случае можно достичь баланса между майнерами и держателями монет, создав систем управления со стороны «внешних» (майнеры) и «внутренних» (держатели) участников. [1] |
| Byzantine fault tolerance (BFT), Byzantine generals problem / Византийская отказоустойчивость, задача византийских генералов | В криптологии - задача взаимодействия нескольких удаленных абонентов, которые получили приказы из одного центра. Часть абонентов, включая центр, могут быть злоумышленниками. Нужно выработать единую стратегию действий, которая будет выигрышной для абонентов. [7] |
| PBFT / Практическая византийская отказоустойчивость | Алгоритм для особого случая и оптимизации византийской отказоустойчивости (BFT). [8] |

Список источников


1. [1] Blockgeeks Inc, «Blockchain Glossary: From A-Z,» [В Интернете]. Available: https://blockgeeks.com/guides/blockchain-glossary-from-a-z.
2. [2] BlockchainTechnologies.com Diversified Internet Holdings LLC, «Blockchain glossary,» [В Интернете]. Available: https://www.blockchaintechnologies.com/glossary/.
3. [3] С. Базанов, «Криптовалюты: Термины и сокращения,» [В Интернете]. Available: https://medium.com/bitcoin-review/bitcoin-криптовалюты-термины-и-сокращения-27293b8413cc.
4. [4] Глоссарий ЕАЭС.
5. [5] Технический комитет по стандартизации Криптографическая защита информации, Термины и определения в области технологий цепной записи данных (блокчейн) и распределенных реестров. МР-26.4.001, Москва, 2018.
6. [6] Федеральный закон «О цифровых финансовых активах», проект.
7. [7] L. Lamport, M. Pease и R. Shostak, «The Byzantine Generals Problem,» ACM Transactions on Programming Languages and Systems 4, т. 3, p. 382—401, 1982.
8. [8] M. Castro и B. Liskov, «Practical Byzantine Fault Tolerance,» Proceedings of the Third Symposium on Operating Systems Design and Implementation, p. 173–186, 1999.

**Лабораторная работа 2**
**Исследование функции обмена файламимежду одноранговыми устройствами**

***Задачи***

***Часть 1. Определение одноранговых сетей, протоколов обмена файлами и приложений***

***Часть 2. Анализ проблем, возникающих при обмене файлами в одноранговых сетях***

***Часть 3. Изучение судебных процессов, связанных с нарушением авторских прав в однораговых сетях***

## *Исходные данные/сценарий*

Одноранговые сети (P2P) —– это мощная технология, которая находит множество областей применения.

Одноранговые сети можно использовать для предоставления общего доступа и обменамузыкой, фильмами, программами и другими электронными материалами.

Использование одноранговых сетей для передачи, загрузки или предоставления общего доступа к материалам, защищённым авторскими правами, таким как фильмы, музыка и программное обеспечение, может нарушать права их владельцев. В контексте обмена файлами в одноранговых сетях нарушение законодательства имеет место в том случае, если, например, один человек приобретает официальную копию файла и выкладывает её затем в одноранговую сеть для общего доступа. В таком случае как лицо, загрузившее файл, так и те лица, которые делают копии, могут быть признаны виновными в нарушении авторских прав и несоблюдении соответствующего законодательства.

Ещё одна проблема заключается в отсутствии достаточной защиты и проверки файлов, которыми обмениваются в одноранговых сетях. Одноранговые сети —– идеальная среда для распространениявредоносного ПО (компьютерных вирусов, червей, троянских программ, шпионских, рекламных и других вредоносных приложений). В 2010 году компания Cisco сообщила о том, что вместе с ростом активности одноранговых сетей появляются и новые вредоносные программы, а значит, обмен файлами в одноранговых сетях получает всё более широкое распространение как среди обычных пользователей, так и среди злоумышленников.

В ходе этой лабораторной работы вы рассмотрите существующее программное обеспечение для обмена файлами в одноранговых сетях и определите, какие проблемы могут возникнуть в результатеиспользования этой технологии.

Часть 1: Определение одноранговых сетей, протоколов обмена файлами и приложений

В части 1 вам необходимо изучить одноранговые сети и узнать, какие протоколы и приложения частоиспользуются для таких сетей.

Шаг 1: Дайте определение одноранговых сетей.

a. Что такое одноранговая сеть?

b. Назовите преимущества одноранговых сетей по сравнению с архитектурой «клиент-сервер».

c. Назовите недостатки одноранговых сетей.

Шаг 2: Дайте определение одноранговых сетей, протоколов обмена файлами и приложений.

a. Укажите, какие протоколы обмена файлами для одноранговых сетей применяются в настоящеевремя.

b. Какие популярные приложения для обмена файлами в одноранговых сетях используютсяв настоящее время?

c. Какой из протоколов для обмена файлами в одноранговых сетях на сегодняшний день считаетсянаиболее популярным в сети Интернет?

Часть 2: Анализ проблем, возникающих при обмене файламив одноранговых сетях

В части 2 вы рассмотрите проблему нарушения авторских прав при использовании одноранговых сетей, а также определите другие спорные моменты, которые могут возникнуть при обмене файламив таких сетях.

Шаг 1: Рассмотрите проблему нарушения авторских прав при использовании одноранговых сетей.

a. Как расшифровывается и что означает сокращение DMCA?

b. Какие две организации активно преследуют нарушение авторских прав в одноранговых сетях?

c. Какое наказание предусмотрено за нарушение авторских прав?

d. Какие законы об авторском праве в отношении обмена файлами действуют в вашей стране? Можно ли назвать их более или менее строгими, чем в других странах? Насколько активно правоохранительные органы в вашей стране преследуют лиц, которые распространяют материалы, охраняемые авторским правом?

Шаг 2: Рассмотрите другие проблемы, связанные с одноранговыми сетями.

a. Какие виды вредоносного ПО могут передаваться путём обмена файлами по одноранговым сетям?

b. Что такое «фальшивые торренты»?

c. Каким образом одноранговые сети могут использоваться для кражи конфиденциальной информации?

Часть 3: Изучение судебных процессов, связанных с нарушениемавторских прав в одноранговых сетях

В части 3 вы рассмотрите некоторые известные судебные процессы по искам о нарушении авторскихправ при использовании одноранговых сетей.

a. Какая известная одноранговая сеть обмена MP3-файлами была закрыта по решению суда?

b. Назовите один из самых крупных судебных процессов, связанных с одноранговыми сетями.

**Лабораторная работа 3**

**Исследование обмена файлами по сетям p2p**

***Задачи***

***Часть 1. Определение сетей p2p, протоколов обмена файлами и приложений***

***Часть 2. Анализ проблем, возникающих при обмене файлами по сетям p2p***

***Часть 3. Изучение судебных процессов, связанных с нарушением авторских прав в сетях p2p***

Общие сведения/сценарий

Одноранговые сети (p2p) — это эффективная технология, которая используется в разных областях. Сети p2p можно использовать для предоставления общего доступа и обмена файлами и другими электронными материалами.

Использование сетей p2p для передачи или загрузки материалов, защищенных авторскими правами, таких как фильмы, музыка и программное обеспечение, может нарушать права их владельцев. В контексте обмена файлами в сетях p2p нарушение законодательства имеет место в том случае, если, например, один человек приобретает официальную копию файла и выкладывает ее затем в одноранговую сеть для общего доступа. В таком случае как лицо, загрузившее файл, так и те лица, которые делают копии, могут быть признаны виновными в нарушении авторских прав и несоблюдении законодательства.

Еще одна проблема заключается в отсутствии достаточной защиты и проверки файлов, которыми обмениваются в сетях p2p. Сети p2p — идеальная среда для распространения вредоносного программного обеспечения (компьютерных вирусов, червей, троянских программ, шпионских, рекламных и других вредоносных приложений).

В ходе этой лабораторной работы вы рассмотрите программное обеспечение для обмена файлами в сетях p2p и определите, какие проблемы могут возникнуть в результате использования этой технологии.

Часть 1: Определение сетей p2p, протоколов обмена файлами и приложений

В части 1 вы изучите сети p2p и узнаете, какие протоколы и приложения часто используются для таких сетей.

Шаг 1: Дайте определение сетей p2p.

a. Что такое сеть p2p?

b. Как минимум два преимущества сетей p2p по сравнению с архитектурой «клиент-сервер».

c. Назовите как минимум два недостатка сетей p2p.

Шаг 2: Дайте определение протоколов обмена файлами по сетям p2p и приложений.

a. Назовите как минимум два протокола обмена файлами по сетям p2p, применяющихся в настоящее время.

b. Назовите как минимум два популярных приложения для обмена файлами по сетям p2p.

c. Какой из протоколов для обмена файлами по сетям p2p на сегодняшний день наиболее популярен в сети Интернет?

Часть 2: Анализ проблем, возникающих при обмене файлами по сетям p2p

В части 2 вы рассмотрите проблему нарушения авторских прав при использовании сетей p2p, а также определите другие проблемы, которые могут возникнуть при обмене файлами в таких сетях.

Шаг 1: Изучите нарушения авторских прав в сетях p2p

a. Как расшифровывается и что означает сокращение DMCA?

b. Какие две организации активно преследуют нарушение авторских прав в сетях p2p?

c. Какое наказание предусмотрено за нарушение авторских прав?

d. Какие законы об авторском праве в отношении обмена файлами действуют в вашей стране? Можно ли назвать их более строгими или менее строгими, чем в других странах? Насколько активно правоохранительные органы в вашей стране преследуют лиц, которые распространяют материалы, охраняемые авторским правом?

Изучите другие проблемы, возникающие при использовании сетей p2p

e. Какие виды вредоносного ПО могут передаваться путем обмена файлами по сетям p2p?

f. Что такое «фальшивые торренты»?

g. Каким образом сети p2p можно использовать для кражи конфиденциальной информации?

Часть 3: Изучение судебных процессов, связанных с нарушением авторских прав в сетях p2p

В части 3 вы рассмотрите некоторые известные судебные процессы по искам о нарушении авторских прав при использовании сетей p2p.

a. Какая известная сеть p2p для обмена MP3-файлами была закрыта по решению суда?

b. Назовите один из самых крупных судебных процессов, связанных с обменом файлами по сетям p2p.

## Расчетно-графическое задание

## Исследование протоколов взаимодействия распределённых реестров

- **План работы:**
- Сценарии применения интероперабельности сетей распределённого реестра.
- Методы интероперабельности распределенных реестров
- Способы реализации интероперабельности платформ
- Практическая реализация технологических решений по интеропеабельности
- Перспективы развития технологических решений по интеропеабельности

Цель – определение практических методов взаимодействия платформ распределенных реестров. Организация интероперабельности выполняется для решения технологических задач: обеспечения конфиденциальности, увеличенияпроизводительности, безопасности и масштабируемости.

**Задачи:**

1. Обзор методов взаимодействия распределенных реестров.
2. Анализ протоколов взаимодействия распределенных реестров, а также зарубежной практики.
3. Разработка сервиса взаимодействия распределенных реестров для платформМастерчейн и Hyperledger Fabric.

### Теоретическая часть

Блокчейн перестал быть технологией будущего: уже сегодня распределенные реестры запускаются в промышленную эксплуатацию, а на рынке присутствуют десятки зрелых решений на блокчейне. Вокруг технологии сформировалось устойчивое сообщество блокчейн-специалистов: только на сервисе GitHub в топ-6 крупнейших блокчейн-платформ для бизнеса зарегистрировано более 30 тыс. разработчиков (Chainstack, 2020).

Технология распределенных реестров активно развивается, однако в экспертном сообществе активно обсуждается ряд нерешенных технологических вызовов. Одиниз них — обеспечение интероперабельности различных блокчейнов. Сегодня, когда использование распределенных реестров предполагает разнообразие и масштабируемость экосистемы, потенциальные преимущества от интероперабельности очевидны:

Наличие большего числа партнеров в рамках блокчейн-экосистемы может повысить ценность и увеличить отдачу от инвестиций в блокчейн

Интероперабельность позволит настраивать и улучшать блокчейн-решения, непозволяя им устаревать.

Интероперабельность это возможность свободного обмена информацией междуразличными блокчейн-системами.

В рамках исследования были изучены интервью с экспертами рынка. Эксперты выразили свое мнение о практических кейсах, препятствиях и перспективах развития функционального взаимодействия платформ распределенных реестров.

С момента запуска биткоина и других альткоинов в ИТ-сообществе стал возникать вопрос функционального взаимодействия платформ для обмена криптовалютой между разными сетями распределенных реестров. Функциональная совместимость (далее – интероперабельность) – это способность двух и более компьютерных систем обмениваться и взаимно использовать полученную информацию (IEC 17788:2014(en) Information technology – Cloud computing – Overview and vocabulary, 2019).

В блокчейн-технологиях под функциональной совместимостью понимают протокол, гарантирующий согласованность логических состояний в двух и более независимых распределенных реестрах. При этом возможные сценарии обмена данными между сетями не ограничиваются обменом только криптовалютой, а включают в себя такжеи решение функциональных задач.

## *ОСНОВНЫЕ СЦЕНАРИИ ПРИМЕНЕНИЯ ИНТЕРОПЕРАБЕЛЬНОСТИ СЕТЕЙ РАСПРЕДЕЛЕННЫХ РЕЕСТРОВ*

### Обмен и передача цифровых активов.

С учетом развития рынка цифровых активов (токенов, криптовалюты) этот сценарий встречается наиболее часто. Процесс обмена и передачи может происходить как с участием доверенной стороны (например, биржи обмена криптовалюты), так и в недоверенной среде с использованием криптографических преобразований для обеспечения безопасности передачи данных. Процесс передачи цифровых активов в недоверенной среде выполняется с использованием смарт-контрактов, которые обеспечивают блокировку токена в одной сети, создание (эмиссию) конвертируемоготокена в другой сети, так что блокированный токен становится недоступным для дальнейших операций

### Обеспечение конфиденциальности данных.

В распределенных реестрах с идентифицированными участниками интероперабельность платформ может использоваться для достижения конфиденциальности данных. Так, например, детальные данные по операциям сделки между ограниченным числом участников записываются в отдельный реестр, которыйхранится только у этих участников.

Масштабируемость и производительность.

Для обеспечения большей скорости распределенный реестр может быть разделен на сегменты (подсети, шарды, сайдчейны). Отдельные операции могут записыватьсяв сегмент сети, при этом результат обработки группы операций записывается в основной реестр.

Функциональное разделение реестров.

Распределенные реестры могут иметь различные смарт-контракты для совершенияразных операций. Например, процесс регистрация цифрового актива может быть выполнен в одном реестре, а его продажа и вторичный рынок — в другом.

Проекты, включающие в себя средства интероперабельности:

Virtualchain, Sidechain, Interledger, Cosmos, Polkadot, Overledger, Token-Bridge, NEARProtocol, Wanchain, BTC Relay, Ethereum 2.0, Corda.

## МЕТОДЫ ИНТЕРОПЕРАБЕЛЬНОСТИ РАСПРЕДЕЛЕННЫХ РЕЕСТРОВ

### *1. ХЕШ-КОНТРАКТЫ ВРЕМЕННОЙ БЛОКИРОВКИ*

Одним из наиболее распространенных способов реализации интероперабельности является атомарный обмен. Он основан на криптографическом протоколе HTLC (Hash Time Locked Contracts) (Hash Time Locked Contracts, 2019). В процессе переносаданных участники обмениваются секретной информацией, которая используется при поверке записи. Примером реализации служит протокол Interledger, поддерживаемыйRipple. Также на основе HTLC построена технология Lightning Network (Lightning Network Documents, 2019), реализация которой выполнена в Мастерчейне для масштабирования количества операций.

Преимущества:

Универсальное решение для всех приложений

Недостатки:

Сервис использует криптографические преобразования (аутентификация, шифрование), требует прохождения сертификации и отдельного ТЗ.

Неустойчив к цензурированию, когда узлы перестают передавать информацию отодной сети в другую.

Требует активного участия взаимодействующих сторон.

## *2. МОСТ НА СТОРОНЕ ДОВЕРЕННОГО УЧАСТНИКА*

Если атомарные обмены и протокол Interledger (Interledger Overview, 2019) подразумевают обмен активами, то мосты подразумевают обмен сообщениями, например, вызов функций смарт-контрактов одного распределенного реестра из другого. Подход основан на наличии в системах посредников (оракулов) для передачиинформации из одного блокчейна в другой.

Преимущества:

Небольшие издержки на настройку программного обеспечения участника. Достаточно проведения оценки влияния на стороне инфраструктуры доверенной организации.

Недостатки:

Требует адаптации для каждого кейса в отдельности исходя из особенностейпередаваемых форматов данных.

Требует поддержки на стороне доверенной организации.

Требует отдельного соглашения между участником и доверенной организацией для каждого кейса в отдельности и включения этой организации в каждый кейс,необходимый для межсетевого взаимодействия.

## *3. РЕЛЕЙНЫЙ БЛОКЧЕЙН (МАСТЕР-СЕТЬ)*

Релейный блокчейн (релейная сеть/мастер-сеть) предполагает создание единой сети из обособленных блокчейн-сетей. При этом согласованность данных блокчейн-сетей,объединенных в релейную сеть, обеспечивается за счет записи их состояний в релейный блокчейн, который лежит в основе такой сети.

Преимущества:

Все изменения выполняются каждым участником независимо. Дополнительная безопасность включенных блокчейнов обеспечивается безопасностью релейной сети.

Недостатки:

Требует прохождения оценки влияния для каждого участника.Решения об инцидентах ИБ не согласованы.

## *СПОСОБЫ РЕАЛИЗАЦИИ ИНТЕРОПЕРАБЕЛЬНОСТИ ПЛАТФОРМ*

## *АТОМАРНЫЙ ОБМЕН*

Реализация атомарного обмена не требует наличия доверенной стороны. При этом

условия его выполнения включают ряд требований:

Пользователи, участвующие в обмене, должны иметь адреса в распределенныхреестрах друг друга.

Платформы не должны в одностороннем порядке ограничивать доступ к сети дляучастников обмена.

Платформы должны поддерживать общие криптографические алгоритмы, чтобы создаваемые криптографические доказательства работали в рамках протокола вразных реестрах. Например, если хеш, блокирующий активы в одном реестре, не подойдет к хешу своего прообраза в другом реестре, то это не позволит вывести активы.

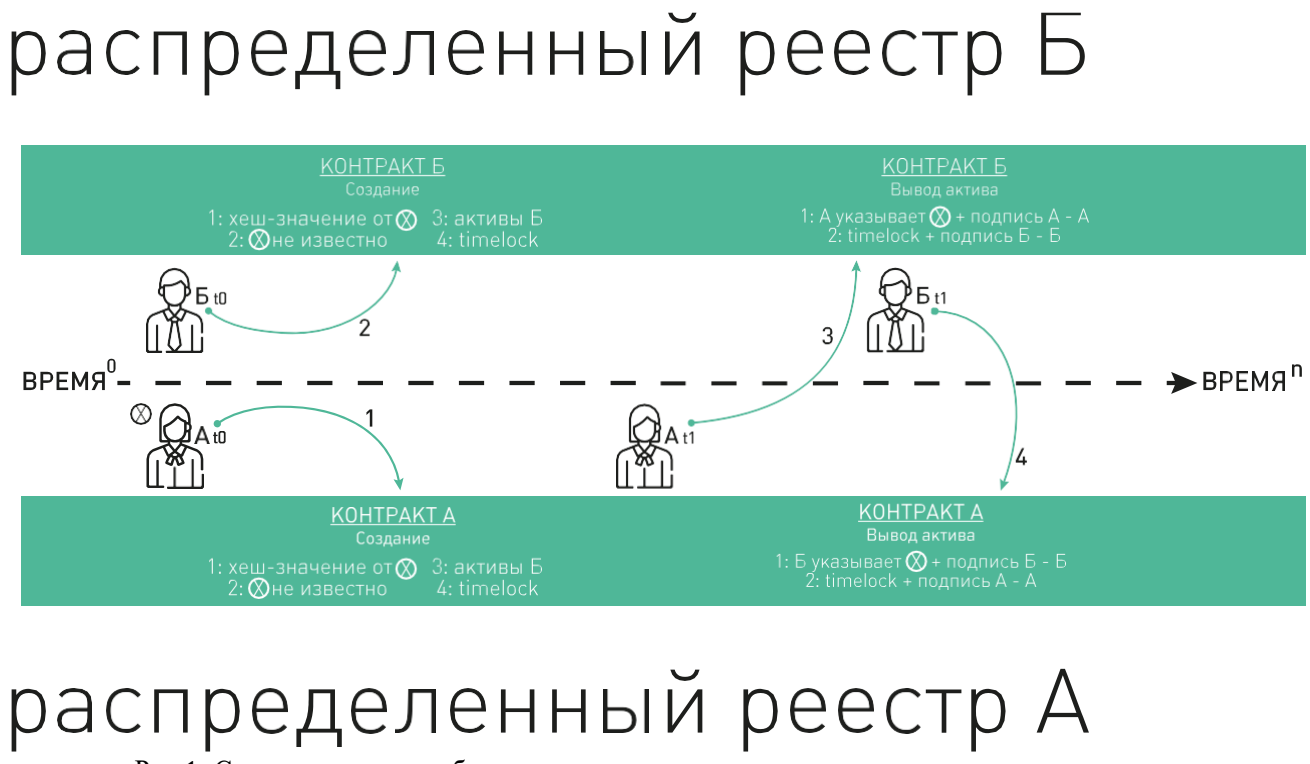



Рис 1. Схема атомарного обмена

**ПОШАГОВОЕ ИСПОЛНЕНИЕ:**

**1.** Алиса придумывает *секрет* и берет от него значение криптографической хеш-функции(далее — *хеш-значение*).

**2.** Алиса размещает в распределенном реестре HTLC-контракт с хеш-значением и блокируетв контракте свои активы для их последующей передачи Борису.

**3.** Алиса передает экземпляр HTLC-контракта с хеш-значением Борису.

**4.** Борис проверяет HTLC-контракт, размещает его в своем реестре и блокирует свои активыдля последующей передачи Алисе.

**5.** Чтобы Алиса забрала активы, заблокированные Борисом, она должна раскрыть секрет,хеш-значение от которого она получила на шаге 1.

**6.** Так как информация хранится публично, Борис видит секрет, который отправила в сеть Алиса, когда забирала свои активы с контракта, размещенного Борисом.

**7.** Борис использует этот секрет, чтобы забрать активы, которые заблокировала Алиса всвоей сети.

**8.** Так как HTLC-контракт подразумевает еще и блокировку по времени, Алиса не может втечение некоторого времени вывести свои активы.

**9.** Борис должен до этого времени вывести активы Алисы, иначе Алиса вернет их себе.

### *МОСТ И НОТАРИАЛЬНАЯ СХЕМА*

Подход «мост» позволяет передавать не только активы, но и сообщения, включаявызов метода смарт-контракта в другом реестре.

В профессиональном сообществе «мостом» называется связка из *сервиса-оракула*, который отслеживает транзакции и события, и *системного смарт-контракта*, который генерирует события внутри своего блокчейна и обрабатывает входящие события из других систем.

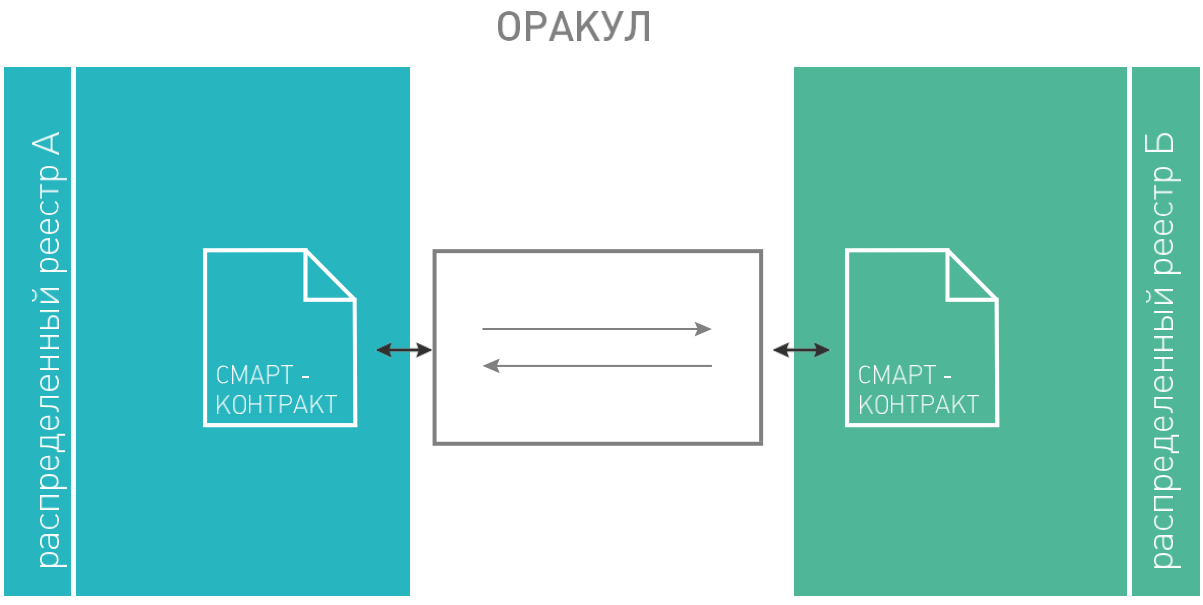


Рис 2. Схема использования моста

Сценарий взаимодействия в сетях на основе Ethereum:

**1.** В смарт-контракте моста вызывается специальный метод, в который передается:адрес вызываемого в другом реестре смарт-контракта,

сигнатура вызываемого метода,
передаваемые в этот метод аргументы.

**2.** Специальный метод генерирует событие, которое содержит информацию,переданную в него на шаге 1.

**3.** *Оракул* прослушивает смарт-контракт моста на наличие новых событий и принаступлении события вызывает связанную с типом события логику, которая выполняет соответствующий метод в смарт-контракте в другой сети.

Мост одновременно размещается в двух сетях, но также может присутствовать только в одной сети, получая всю необходимую информацию по другим каналам связи. При этом основная функция заключается в криптографический проверки аутентичности передаваемой информации взаимодействующих участников.

Нотариальные схемы являются развитием подхода типа «мост». Главный элемент нотариальных схем — т. н. «нотариусы»: они несут ответственность за передачу сообщений, и чаще всего именно им отведена роль валидаторов в блокчейн-сети. Обязанности нотариусов — проверка того, что событие было сгенерировано в одном распределенном реестре, сбор необходимых подтверждений о событии от других участников нотариальной схемы и передача информации о событии в другой реестр.

## *РЕЛЕЙНЫЙ БЛОКЧЕЙН, ИЛИ МАСТЕР-СЕТЬ*

Релейный блокчейн (мастер-сеть) — это отдельный многоуровневый блокчейн, который связывает обособленные блокчейн-сети в единую структуру. Возможностьпроверить и передать данные из одного блокчейна в другой через связующий«релейный» блокчейн называется релейной передачей.

Релейный блокчейн наблюдает за состояниями всех связанных в релейную сетьблокчейнов и при необходимости, согласно определенным правилам, может контролировать и управлять активами в этих сетях.


Рис 3. Релейная сеть, или мастер-сеть

В рамках подхода «релейный блокчейн» стоит упомянуть о т. н. *сайдчейне*. Сайдчейн(от англ. sidechain – боковая цепь) – это обособленный блокчейн, который входит в структуру релейной блокчейн-сети. В зависимости от реализации сайдчейны имеют различную степень зависимости от своего «родительского» блокчейна.

Основная цель сайдчейнов – реализация возможности безопасного перемещения некоторых цифровых активов между реестрами для проведения действий над ними.

Предпосылки для использования подхода «сайдчейн»:

Время подтверждения транзакций. Задержки транзакций в сайдчейне обычно значительно меньше, чем в основном блокчейне.

Стоимость записи транзакций. В сайдчейне стоимость транзакций может бытьзначительно ниже, чем в основном блокчейне.

Расширение функциональных возможностей. Сайдчейн может обладать некоторыми функциональными возможностями, которые могут отсутствовать в основном блокчейне.

В настоящее время релейный блокчейн проходит стадию исследований и не рассматривается.

СРАВНЕНИЕ ПОДХОДОВ

| | Атомарный обмен | Построение моста | Релейная цепь |
|---|---|---|---|
| Назначение | Передача активов | Передача сообщений | Передача сообщений |
| Масштабируемость по количеству участников | Низкая | Средняя | Высокая |
| Требуется доверенный участник | Нет | Да | Нет |
| Сложность реализации | Низкая | Средняя | Высокая |
| Отношения между участниками обмена | Один-к-одному | Один-к-одному | Многие-ко-многим |
| Способ обеспечения достоверности данных | Криптографическиепреобразования | Выделенный участник | Доверенная сеть |
| Примеры реализации | Interledger, LightningNetwork | Corda, BTC Relay, TokenBridge, Overledger | Polkadot, Cosmos, Ethereum 2.0, NEAR Protocol, Wanchain,Sidechain |

# ОБЗОР ЗАРУБЕЖНЫХ ПРОЕКТОВ ИНТЕРОПЕРАБЕЛЬНОСТИ

На фоне постоянного развития отрасли и растущей необходимости в налаживаниисовместимости между различными блокчейн-сетями уже появились различные примеры работы над соответствующими решениями. С одной стороны, наличие таких игроков свидетельствует о развитии рынка, с другой — инициативы довольно конкретные и работают только с определенными платформами.

## *POLKADOT*

Идея Polkadot приписывается Гэвину Вуду, одному из сооснователей Ethereum. Polkadot облегчает не только транзакции, но и обмен данными. Экосистема Polkadot содержит парачейны (parachains — отдельные блокчейны,

ставшие частью среды Polkadot) и релейную цепь (relay chain), которая их соединяет. Каждый парачейн может иметь различные характеристики и распространять свои транзакции по всей экосистеме. Все цепочки, которые становятся частью экосистемы Polkadot, должны адаптировать свои механизмы консенсуса к правилам Polkadot, но у них есть свободаразвития структуры и функций своего блокчейна.

### *BLOCKNEl'*

Blocknet — это протокол для совместимости, который обеспечивает связь, взаимодействие и обмен данными между различными публичными и частными блокчейнами, а также доступ к внесетевым данным, API и сервисам через оракулов

### *ARK*

Ark ставит своей целью создание масштабируемого и адаптируемого решения для взаимодействия с блокчейном. Компания автоматизировала создание новых блокчейнов в экосистеме. Платформа Ark имеет встроенную поддержку для многих языков программирования, включая Java, Swift, Python и Ruby. Это делает ее доступной для людей, которые предпочитают работать с определенными языками.

### *WANCHAIN*

Wanchain позиционирует себя как первое в мире интерактивное блокчейн-решение с защищенными многопользовательскими вычислениями. В его основе лежит Ethereum, который позволяет развертывать смарт-контракты. Также Wanchain позиционируетсякак блокчейн-решение для создания распределенных приложений, которые требуют легкого доступа к различным блокчейнам. Конфиденциальность на блокчейне повышается за счет использования одноразовых скрытных адресов и кольцевых подписей (вид электронной подписи, который позволяет одному из участников группыподписать сообщение от имени всей группы, сохранив при этом свою анонимность).

### *COSMOS*

Cosmos в настоящее время является одной из крупнейших инициатив по обеспечению совместимости блокчейн-платформ. Эта экосистема работает по алгоритму консенсуса Tendermint. Независимые блокчейны, называемые зонами, подключаются к сети Cosmos, при этом все зоны связаны с Cosmos Hub и могут взаимодействовать друг с другом.

### *BLOCKCHAIN IN|'EROPERABILII'Y ALLIANCE*

Blockchain Interoperability Alliance — это объединение ICON, Aion и Wanchain. Альянс уже начал сотрудничать в области исследования обменных операцийи коммуникаций. Разработка общих отраслевых стандартов, а также обмен

результатами исследований и архитектурой протоколов остаются на повестке дня напервом месте.

### *INl'ERLEDGER*

Interledger – это набор открытых протоколов для отправки платежей между различными реестрами. Выпущен компанией Ripple в 2015 году.

### *LIGHl'NING NEl'WORK*

Lightning Network – это децентрализованная система мгновенных микроплатежей(менее нескольких центов – до 0,00000001 биткоина).

### *CORDA SEl'l'LER*

Corda Settler – приложение консорциума R3 с открытым исходным кодом для проведения международных платежей. Первым токеном, поддерживаемым CordaSettler, стал XRP от Ripple.

### *Bl'C RELAY*

BTC Relay позволяет смарт-контрактам на Ethereum безопасно проверять транзакции биткоинов без посредников: пользователи могут платить биткоинами для использования Ethereum DApps.

### *l'OKENBRIDGE*

TokenBridge позволяет обмениваться данными (например, информацией о владениицифровым активом) между двумя цепями в экосистеме Ethereum. В режиме бета-тестирования разработаны три моста между Ethereum Mainnet и другими сетями, построенными на Ethereum: POA, xDai, Eth Classic. Также тестирование проходят мосты Arbitrary Message (для обмена любыми данными между любыми цепями, основанными на Ethereum Virtual Machine) и ETH-BNC (Ethereum to Binance).

### *OVERLEDGER*

Overledger – это операционная система для блокчейна, которая позволяет приложениям подключаться к нескольким технологиям распределенного реестра или блокчейна, тем самым превращаясь в «многоцепочные» приложения (англ. multi-chain applications, mApps). Разработчики могут создавать подписанные транзакции и отправлять их одновременно всем поддерживаемым технологиям распределенного реестра через интерфейс Blockchain Programming Interface (BPI) Overledger.

### *El'HEREUM 2.0*

На июль 2020 года запланирован выход Ethereum 2.0. Для обновления под названием Istanbul (хардфорк состоялся в декабре 2019 года) в числе предложений

EIP (EthereumImprovement Proposals) было вынесено EIP-152. Его суть в том, что внедряется новый контракт с целью создания интероперабельности между виртуальной машиной Ethereum (EVM) и ZCash или другими криптовалютами на базе протокола Equihash.

### *NEAR PROl'OCOL*

NEAR — управляемая сообществом разработчиков облачная инфраструктура для развертывания и запуска децентрализованных приложений. Она сочетает в себе функции децентрализованной базы данных с другими функциями бессерверной вычислительной платформы. Токен, который позволяет этой платформе работать,также дает возможность приложениям, построенным поверх нее, легко взаимодействовать друг с другом.

### *EN\'ERPRISE El'HEREUM ALLIANCE (EEA)*

Альянс EEA запустил в январе 2020 года песочницу EEA TestNet, где форки Ethereum могут быть стандартизированы в соответствии с определенными спецификациями, установленными ранее альянсом, что сделает их совместимыми друг с другом. В настоящее время сотни компаний работают над корпоративными версиями Ethereum, появляются новые игроки, присоединившиеся к альянсу через Hyperledger Besu (Ethereum — участник консорциума Hyperledger), что делает стандартизацию приоритетом.

### *JASPER-UBIN*

В ходе совместного проекта денежно-кредитного управления Сингапура и БанкаКанады были объединены распределенные реестры двух государств — Project Ubin и Project Jasper. Пилотный проект доказал возможность успешного обмена токенизированных цифровых валют между разными блокчейн-платформами. В основе лежал подход HTLC. Эксперимент проводился на платформах Quorum (сингапурский Project Ubin) и Corda (канадский Project Jasper). В ходе проекта были переведены 105 сингапурских долларов из местного банка в канадский с валютным курсом 1 сингапурский доллар к 0,95 канадскому доллару. В итоге канадский банк получил 100 сингапурских долларов.

## ПРАКТИЧЕСКАЯ РЕАЛИЗАЦИЯ НА ПРИМЕРЕ ПЛАТФОРМ МАСТЕРЧЕЙН И HYPERLEDGER FABRIC

Исследуемые подходы, обеспечивающие интероперабельность сетей Мастерчейни Hyperledger Fabric: атомарный обмен, HTLC-протокол. Подход

выбран из-за простоты программной реализации и концепции обмена активами между идентифицированными участниками в разных сетях.

Построение моста между сетями Мастерчейн и Hyperledger Fabric. Подход «мост»выбран из-за возможности передачи произвольных сообщений между сетями, которые можно использовать для вызова функции смарт-контрактов в других реестрах и возврата данных в вызывающий смарт-контракт.

Прикладной целью исследований было изучение этих подходов и определение потенциальных проблем и трудностей реализации интероперабельности междусетями Мастерчейн и Hyperledger Fabric.

Сопутствующей целью было определение и понимание границ применимости технологий Burrow EVM (EVMCC) (Hyperledger Burrow — Hyperledger, 2019) при создании атомарного обмена и моста между сетями. Выбор технологий Burrow EVMи EVMCC был обусловлен их технологической близостью к платформе Мастерчейн.

## ОПИСАНИЕ ИСПОЛЬЗУЕМЫХ ТЕХНОЛОГИЙ

Мастерчейн (v1.0) – сертифицированный распределенный реестр, основанный на платформе Ethereum и созданный для проведения юридически значимых транзакций.Разработан Ассоциацией ФинТех совместно с ключевыми участниками российского финансового рынка.

Solidity 0.5.x – язык написания смарт-контракта для EVM и компилятор, которыйпреобразует исходный код в байт-код EVM.

Hyperledger Fabric (v1.4) — фреймворк для создания доверенных корпоративныхраспределенных реестров с алгоритмом консенсуса (класса CFT) Raft (The Raft Consensus Algorithm, 2019). Далее используется аббревиатура HLF. Типовое использование HLF заключается в создании закрытой сети, в которой организации-участники генерируют и обрабатывают транзакции. За упорядочивание и распространение транзакций отвечает ключевой элемент сети — узлы Ordering Service. Участвующие в бизнес-процессах организации формируют каналы, в которыхпроисходит их взаимодействие. Бизнес-логика взаимодействия осуществляется через предварительно размещенные в канале чейнкоды.

Hyperledger Burrow – проект консорциума Hyperledger, целью которого является реализация спецификации Ethereum под управлением консенсуса Tendermint (Tendermint Docs, 2019).

EVMCC — чейнкод для канала в сети Hyperledger Fabric. Работа чейнкода EVMCC заключается в создании внутри себя окружения Burrow EVM, в котором можно запустить смарт-контракт и вызвать его бизнес-логику. После размещения и инициализации чейнкода в канале к нему можно обращаться как к экземпляру EVM иразмещать в нем смарт-контракты.

В нашем исследовании мы размещаем смарт-контракты атомарного обмена (HTLC. sol) и моста (Bridge.sol) в сети Мастерчейн и чейнкоде EVMCC (Hyperledger Fabric).

### *ПОДХОД «АТОМАРНЫЙ ОБМЕН»*

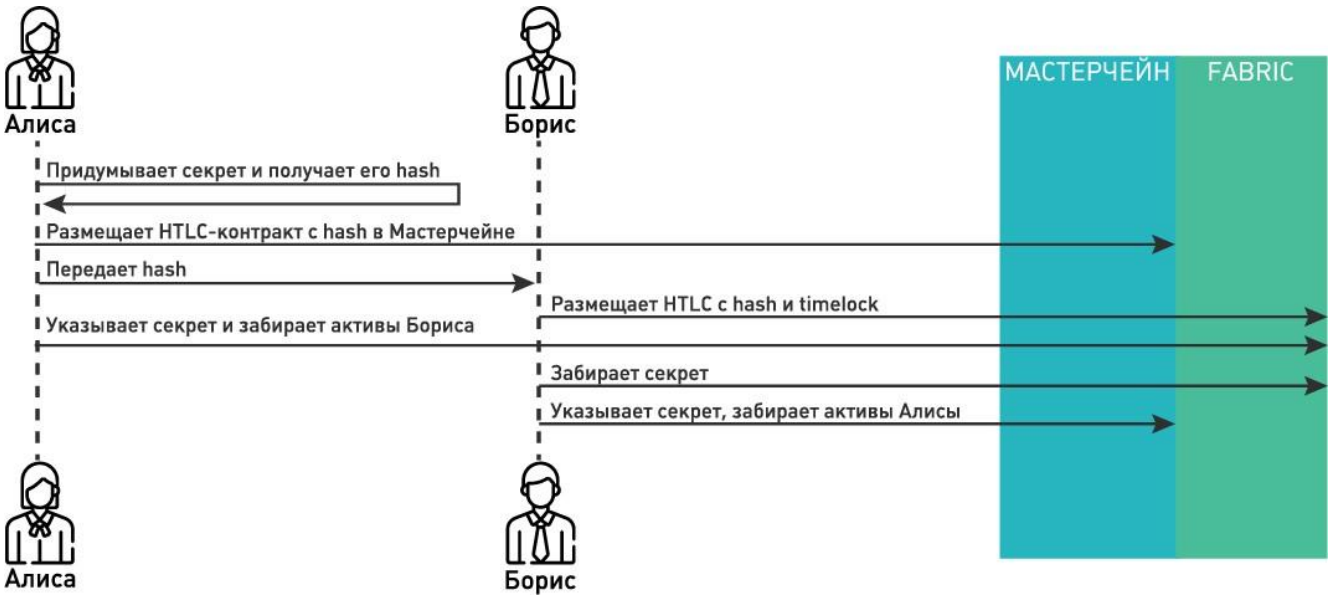



Рис.4 Диаграмма последовательности схемы «атомарный обмен»

Атомарный обмен включает в себя смарт-контракты, размещенные в сетях Мастерчейн и Hyperledger Fabric, и дальнейшее выполнение HTLC-протокола с их участием.

Экземпляр основной структуры данных атомарной сделки

```
struct HushTimeLockContract {
        adress payble sender; // адрес отправителя платежа
        adress payble receiver; // адрес получателя платежа
        uint amount; // количество передаваемых активов
        bytes32 hashlock; // хеш-значение от прообраза
        unit timelock; // Врема UNIX в секундах, блокировка во времени
        bool withdrawn; // логическое поле - были ли активы выведены
        bool refunded; // логическое поле - были ли активы возвращены
        bytes32 preimage; // прообраз для hashLock, по умолчанию 0x0
    }
```

### *РЕАЛИЗАЦИЯ СЦЕНАРИЯ*

1. Смарт-контракт HTLC_A.sol размещается в сети Мастерчейн.
2. Алиса загадывает секрет (*preimage*) и берет от него хеш-значение (*hashlock*).
3. Алиса вызывает метод newContract у размещенного в сети

Мастерчейн смарт контракта HTLC_A.sol и передает в него параметры (receiver – *получатель_активов*, hashlock, timelock – *время_жизни_контракта*) и создает тем самым новую сделку наколичество активов переданных в *msg.value.*

**4.** Борис размещает аналогичный контракт (HTLC_B.sol) в своей сети HLF и указываетсвои данные, но hashlock берет у Алисы.

**5.** Алиса, чтобы перевести активы себе на счет в реестре Бориса (HLF), должна вызвать функцию смарт-контракта HTLC_B *withdraw* и указать *preimage* — после этого активы будут переведены на ее счет, а *preimage* будет записан в реестре HLF.

**6.** После того как *preimage* Алисы будет записан в HLF, Борис может увидеть его и воспользоваться им для перевода активов в реестре Алисы (Мастерчейн), вызвавфункцию *withdraw* в HTLC_A.

**7.** Алиса получила активы в реестре Бориса (HLF), Борис получил активы в реестреАлисы (Мастерчейн). Сделка совершена.

## *ПОДХОД «ПОСТРОЕНИЕ МОСТА МЕЖДУ СЕТЯМИ»*

Реализация подхода типа «мост» заключается в размещении в сетях Мастерчейн иHLF системных смарт-контрактов и создании сервиса-оракула.

Реализация подхода типа «мост» заключается в размещении в сетях Мастерчейн иHLF системных смарт-контрактов и создании сервиса-оракула.

Основная задача системных смарт-контрактов заключается в регистрации события вызова прикладного смарт-контракта, расположенного в другом реестре. Зарегистрированное событие является триггером для выполнения логики сервиса-оракула.

Сервис-оракул – это программа, которая отслеживает активность системных смарт- контрактов. При возникновении в системных смарт-контрактах событий оракул выполняет связанную с типом события логику. В нашем случае – вызов функций в другом реестре.

}

Например, при вызове функции системного смарт-контракта *setValueInAnotherBC* регистрируется событие *RequestForChangeValue* (которое содержит передаваемые данные в специальном формате), оракул получает это событие из логов Мастерчейна,проверяет корректность поступившей информации в Hyperledger Fabric (адреса

смарт-контрактов, адреса участников, соответствие отправляемых и принимаемых данных, подписи транзакций), после чего вызывает соответствующую функцию прикладного смарт-контракта в запрашиваемом реестре.

Прикладные смарт-контракты — это смарт-контракты, функции которых мы вызываемиз других реестров, или контракты, в которых мы вызываем функции других смарт- контрактов в других распределенных реестрах.

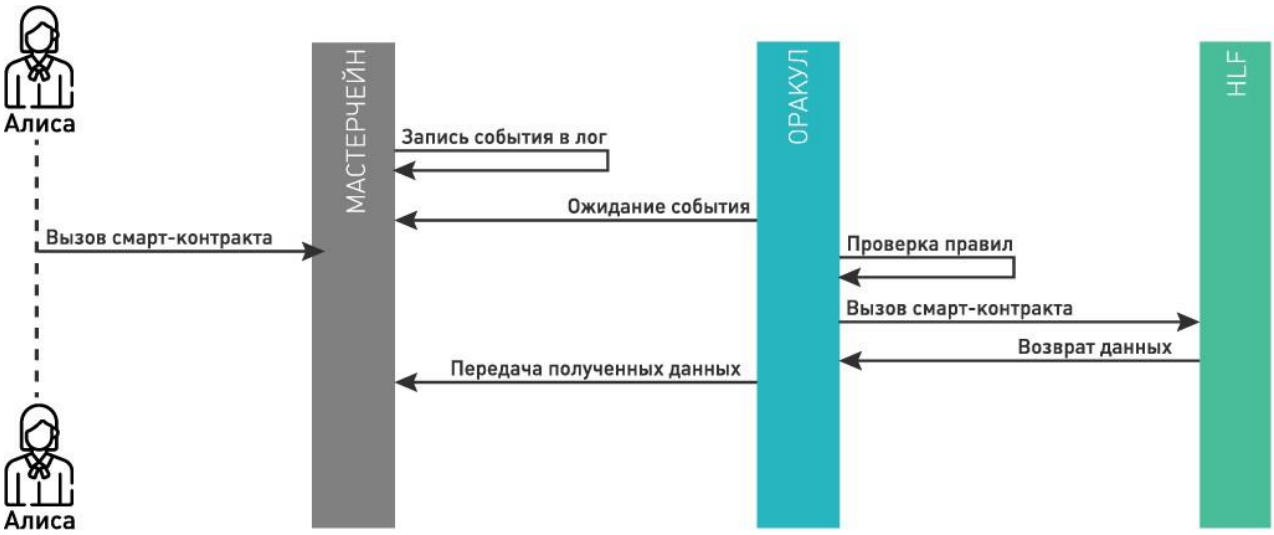



Рис 5. Диаграмма последовательности взаимодействия через мост

**1.** реестрах Мастерчейн и HLF размещается системный смарт-контракт Bridge.sol.

**2.** В реестрах Мастерчейн и HLF размещаются прикладные смарт-контрактыTestMasterchain.sol и TestHLF.sol.

**3.** Алиса (реестр Мастерчейн) хочет вызывать функцию setValue в смарт-контрактеTestHLF (реестр HLF) и передать в нее данные.

**4.** Алисе известен адрес смарт-контракта TestHLF, функцию которого ей нужно вызвать, и ей известна сигнатура вызываемой функции в виде первых 4 байтов.

**5.** Алиса (Мастерчейн) вызывает в смарт-контракте Bridge.sol функциюsetValueInAnotherBC

**6.** Функция setValueInAnotherBC кодирует поступившую информацию о методе (4байта сигнатуры) и передаваемых в него данных.

**7.** Функция setValueInAnotherBC формирует событие, передает в него адрес вызываемого смарт-контракта, закодированные данные и затем записываетсобытие в логи смарт-контракта Bridge.

**8.** Оракул подписан на события смарт-контракта Bridge, и при возникновении новогособытия он определяет адрес и функцию вызываемого смарт-контракта.

**9.** Оракул вызывает функцию в смарт-контракте в сети HLF и передает в негоотправленные Алисой данные.

**10.** После проверок на корректность и доступ данные записываются в реестр HLF.

**11.** Оракул возвращает Алисе хеш-транзакции как подтверждение проведеннойоперации.

### *ВЫВОДЫ ПО ПРАКТИЧЕСКОЙ ЧАСТИ*

### *АТОМАРНЫЙ ОБМЕН*

Реализация EVMCC для HLF не хранит пользовательские адреса на уровне состояния распределенного реестра, а генерирует их на основе публичных пользовательских ключей сети HLF. Соответственно, нет балансов и встроенной платежной единицы, которая могла бы быть заблокирована контрактом HTLC. В качестве альтернативы можно рассмотреть реализацию токенов на основе протокола ERC-20. Совмещая базовую реализацию HTLC и ERC-20, можно создать комбинированный контракт, который позволяет выполнить перевод токенов из одной сети в другую.

Из-за несовместимости используемой платформами криптографии в EVMCC невозможно проверить результат хеширования прообраза для разблокировки активов. Эта фундаментальная для HTLC проблема не позволяет реализовать атомарный обмен между сетями Мастерчейн и HLF.

### *ВЫЗОВ ФУНКЦИЙ ЧЕРЕЗ МОСТ*

При проведении испытаний на стороне EVMCC обнаружено, что транзакции не содержат vrs (ECDSA: (v, r, s), what is v?, 2019), по которым возможно однозначноопределить отправителя транзакции, проверив подпись транзакции. Эта особенность мешает строить безопасное взаимодействие между сетями.

### *ОСОБЕННОСТИ EVMCC/BURROW*

EVMCC — это не отдельный экземпляр Burrow EVM, а представление Burrow EVMв среде Hyperledger Fabric в виде чейнкода, который оказался недостаточно функциональным для реализации выбранных подходов. Например, в EVMCC отсутствуют аккаунты (адреса, балансы, платежные единицы, трансфер платежныхединиц), в Burrow не реализованы некоторые предкомпилированные смарт- контракты ([SNatives] Implement mainline Ethereum precompiles, 2019). В HLF Burrow используется криптография, отличная от той, которая используется в Мастерчейне – это накладывает ряд ограничений на реализацию интероперабельности платформ.

## ПЕРСПЕКТИВЫ РАЗВИТИЯ ТЕХНОЛОГИЧЕСКИХ РЕШЕНИЙ ПО ИНТЕРОПЕРАБЕЛЬНОСТИ

По консолидированному мнению опрошенных экспертов, необходимость в интероперабельности есть, но рынок еще недостаточно осознал ее. Это связано со слабой развитостью рынка блокчейн-решений в целом и отсутствием промышленных сетей, которые можно было бы объединить для создания «сквозных» бизнес-процессов. При этом эксперты сходятся во мнении, что подходы к интероперабельности необходимо исследовать и развивать, так как потребность в функциональной совместимости будет нарастать — это связано с активным развитиемтехнологий распределенных реестров и вводом блокчейн-решений в промышленную эксплуатацию.

Некоторые эксперты считают, что будущее – за консорциумными блокчейн-сетями, которые свяжут в общее информационное пространство организации, объединенныепо сфере профессиональной деятельности или сектору экономики. Такие сетибудут представлять из себя кластеры с выделенной структурой управления. Функциональное взаимодействие подобных кластеров потенциально можетреализовать концепцию Internet-of-Value (Internet of Value Manifesto, 2019).

Ричард Браун, технический директор блокчейн-консорциума R3, предлагает разбить проблему интероперабельности на конкретные составляющие, чтобы эффективнее ее решать (Brown, 2020):

нужна *интеграция* с существующими системами;
нужна возможность *инициировать* транзакции на других сетях;

нужна возможность осуществлять *interchain*-транзакции (между разными реестрами) с решениями на других технологиях;

нужна возможность проводить *intrachain*-транзакции (с использованием различныхвариантов развертывания одной и той же технологии);

нужно упростить *interchange* – замену одной базовой платформы на другую.

Также эксперты сходятся во мнении, что функциональная совместимость распределенных реестров, основанных на различных технологиях, придает значительную ценность платформам с функциями интероперабельности.

Интероперабельность позволит реализовать новые бизнес-кейсы в консорциумных и частных распределенных реестрах. При этом у экспертов нет единого мнения относительно возможного успеха функционального взаимодействия открытых (публичных) блокчейнов и консорциумных распределенных реестров. Среди причин, по которым возникли сомнения в успехе, — разные функциональные свойства, требования к безопасности и производительности.

Главными препятствиями для развития технологий интероперабельности являются: ключевые расхождения в используемых технологиях (различия в классах консенсусов, криптографическая несовместимость, разные способы обработки транзакций), недостаточность научных и практических исследований

технологий подобного рода, отсутствие острой потребности в интероперабельности, дефицит профессиональных стандартов в сфере функционального взаимодействия распределенных реестров.

По мнению экспертов, подходы к интероперабельности необходимо стандартизировать, но процессы стандартизации необходимо выполнять после апробации подходов на реальных кейсах, которые позволят сформировать практические требования.

Стоит отметить, что в данный момент ведутся исследования в международных центрах стандартизации: в International Organization for Standardization, ISO/TC 307 Blockchain and distributed ledger technologies (Международная организация по

стандартизации, ИСО/ТК 307 «Блокчейн и технологии распределенного реестра»), в International Telecommunication Union, ITU-T (Международный союз электросвязи, Сектор стандартизации электросвязи – МСЭ-Т). На национальном уровне – в

Техническом комитете по стандартизации «Криптографическая защита информации» (ТК 26) и в Техническом комитете по стандартизации «Программно-аппаратные средства технологий распределенного доступа и блокчейн» (ТК 159).

Ждет ли нас в будущем огромное количество блокчейн-платформ? Скорее всего, нет. Уже сейчас есть топ-3 платформы, занимающие значительную долю рынка: Ethereum, Hyperledger и Corda. Если три года назад отрасль находилась в состоянииповышенного внимания к технологии, то к настоящему времени рынок значительно созрел в технологическом плане, и пришло время для следующего шага в развитии технологии — обеспечения взаимодействия между разными платформами. Поэтому будущее — не за большим количеством платформ, а за протоколами для их взаимодействия и стандартизацией.

# ЗАКЛЮЧЕНИЕ

Распределенные реестры сталкиваются с непростой задачей: обеспечить интероперабельность между сетями в условиях недостатка доверия к согласованности данных и обеспечения безопасности каналов связи.

В зависимости от требований подходы к интероперабельности имеют разный уровень сложности реализации: от криптографической связи транзакций в различных реестрах до многоуровневых структур с высокой степенью масштабируемости.

При этом у всех подходов прослеживаются общие ограничения.

## *СОГЛАСОВАНИЕ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ*

Основная задача при разработке протоколов функциональной совместимости – согласование криптографических алгоритмов, которые будут использоваться припередаче информации и взаимодействия систем.

Важными факторами при согласовании логических состояний объединяемых реестров являются: противодействие «недобросовестному» поведению, отсутствие единой точки отказа, существующие политики доступа и управления распределенными реестрами.

## *СТАНДАРТИЗАЦИЯ*

Стандарты для обеспечения безопасной интероперабельности распределенных реестров еще не разработаны рынком. При этом рынок понимает, что стандартизация подходов к интероперабельности неизбежна. Решением этих вопросов занимаются в техническом комитете 159 «Программно-аппаратные средства технологийраспределенного реестра и блокчейн» рабочие группы «Интеллектуальные контракты» и «Взаимодействие систем распределенных реестров».

Участие представителей рынка в процессах стандартизации подходов, протоколов, концепций обеспечения функциональной совместимости распределенных реестров поможет решить ряд будущих организационных и технических вопросов.

## *ПРИОРИТЕТНЫЕ ПОДХОДЫ В КОРПОРАТИВНОМ СЕКТОРЕ*

Подход «мост» предполагается рассматривать как наиболее применимый для использования в корпоративной среде.

Во-первых, этот поход обеспечивает возможности передачи структурированных сообщений.

Во-вторых, с учетом идентификации участников может быть выбрана доверенная сторона или нотариат.

В-третьих, подход обеспечивает должный уровень конфиденциальности соединяемых распределенных реестров с учетом относительной простоты реализации.

Релейная сеть (мастер-сеть) потенциально позволит объединить распределенные реестры в единую сеть, повысив безопасность включенных в нее распределенных реестров и упростив передачу сообщений между ними посредством использования общих криптографических алгоритмов. Это направление интероперабельности активно исследуется, но на данный момент ни одно из решений в рамках релейной сети не прошло достаточных промышленных испытаний.

### *ИНТЕРОПЕРАБЕЛЬНОСТЬ МАСТЕРЧЕЙНА*

Платформа Мастерчейн продолжит исследования и свое развитие в сторону использования подхода типа «мост». Этот подход обладает необходимыми свойствами, которые обеспечивают должный уровень безопасности, конфиденциальности и гибкости при взаимодействии с внешними информационнымисистемами и иными распределенными реестрами

## КЛЮЧЕВЫЕ ВЫВОДЫ ИССЛЕДОВАНИЯ

Сегодня рынок блокчейн-платформ фрагментирован: отсутствуют единые стандарты, которые позволяли бы беспрепятственно обмениваться информацией между различными распределенными реестрами.

Эксперты в области блокчейна ставят задачу обеспечить интероперабельность между различными сетями в условиях отсутствия доверия к согласованности данных в системах обеспечения выполнения безопасности каналов связи.

Один из ключевых факторов обеспечения интероперабельности – согласованиекриптографических алгоритмов, которые будут использоваться при передаче информации и взаимодействии систем.

Индустрия еще не разработала стандарты для обеспечения безопасной интероперабельности распределенных реестров. При этом участникам рынка становится очевидной необходимость стандартизации подходов к интероперабельности.

Участие представителей рынка в процессах стандартизации подходов, протоколов и концепций поможет решить ряд будущих организационных и технических вопросов.

Сегодня существуют различные методы обеспечения интероперабельности распределенных реестров. Мы считаем, что описанный ниже подход «мост» наиболее применим для использования в блокчейн-решениях для бизнеса.

Платформа Мастерчейн продолжит исследования и свое развитие в сторону использования подхода типа «мост». Этот подход обеспечивает должный уровень безопасности, конфиденциальности и гибкости при взаимодействии с внешними информационными системами и иными распределенными реестрами.

## 10 Описание материально-технического обеспечения, необходимого для осуществления образовательного процесса по дисциплине (модулю)

### 10.1 Учебно-лабораторное оборудование

Таблица 8 – Перечень оборудования лаборатории

| Аудитория | Наименование аудитории (лаборатории) | Используемое оборудование |
|---|---|---|

| | | |
|---|---|---|
| 201/5 | Учебная лаборатория защищённых автоматизированных систем | СЗИ НСД Secret Net, СЗИ НСД Dallas Lock, СЗИ НСД Страж NT, СЗИ НСД Щит РЖД, СЗИ НСД Аура ,СЗИ НСД Криптон ,СЗИ НСД Аккорд, ФИКС, Ревизор 1,2 как для операционных систем семейства Windows так и для Linux, Ревизор Сети 2.0, Анализатор сетевого траффика Астра,Агент инвентаризации сети,Сканер сетевой безопасности XSpider, Терьер, Secret Net Touch Memory Card, Криптон АМДЗ, Аккорд АМДЗ, КриптоПРО АРМ, ,CryptoPro CSP 3.6, VipNet firewall, Etoken PKI Client, Etoken, Ноутбук с Windows 7+проектор.<br>16 ПЭВМ на базе процессоров не ниже Intel Pentium IV |

### 10.2 Технические и электронные средства обучения

**Лекционные занятия**

Аудитории для лекционных занятий укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории (наборы демонстрационного оборудования (проектор, экран, компьютер/ноутбук), учебно-наглядные пособия, тематические иллюстрации).

**Лабораторные занятия**

Для лабораторных занятий используется аудитория № 201 , оснащенная оборудованием, указанным в табл. 8:

**Самостоятельная работа**.

Помещения для самостоятельной работы оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде КнАГУ:

- читальный зал НТБ КнАГУ;
- компьютерные классы (ауд. 311 корпус № 5, ауд. 205 корпус № 5, ауд. 313 корпус № 5).

## 11 Иные сведения

**Методические рекомендации по обучению лиц с ограниченными возможностями здоровья и инвалидов**

Освоение дисциплины обучающимися с ограниченными возможностями здоровья может быть организовано как совместно с другими обучающимися, так и в отдельных группах. Предполагаются специальные условия для получения образования обучающимися с ограниченными возможностями здоровья.

Профессорско-педагогический состав знакомится с психолого-физиологическими особенностями обучающихся инвалидов и лиц с ограниченными возможностями здоровья, индивидуальными программами реабилитации инвалидов (при наличии). При необходимости осуществляется дополнительная поддержка преподавания тьюторами, психологами, социальными работниками, прошедшими подготовку ассистентами.

В соответствии с методическими рекомендациями Минобрнауки РФ (утв. 8 апреля 2014 г. N АК-44/05вн) в курсе предполагается использовать социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе.

Подбор и разработка учебных материалов производятся с учетом предоставления материала в различных формах: аудиальной, визуальной, с использованием специальных технических средств и информационных систем.

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения (персонального и коллективного использования). Материально-техническое обеспечение предусматривает приспособление аудиторий к нуждам лиц с ОВЗ.

Форма проведения аттестации для студентов-инвалидов устанавливается с учетом индивидуальных психофизических особенностей. Для студентов с ОВЗ предусматривается доступная форма предоставления заданий оценочных средств, а именно:

· в печатной или электронной форме (для лиц с нарушениями опорно-двигательного аппарата);

· в печатной форме или электронной форме с увеличенным шрифтом и контрастностью (для лиц с нарушениями слуха, речи, зрения);

· методом чтения ассистентом задания вслух (для лиц с нарушениями зрения).

Студентам с инвалидностью увеличивается время на подготовку ответов на контрольные вопросы. Для таких студентов предусматривается доступная форма предоставления ответов на задания, а именно:

· письменно на бумаге или набором ответов на компьютере (для лиц с нарушениями слуха, речи);

· выбором ответа из возможных вариантов с использованием услуг ассистента (для лиц с нарушениями опорно-двигательного аппарата);

· устно (для лиц с нарушениями зрения, опорно-двигательного аппарата).

При необходимости для обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.

Приложение 1

# ФОНД ОЦЕНОЧНЫХ СРЕДСТВ[1]
# по дисциплине
# Обеспечение информационной безопасности в пиринговых сетях

| | |
|---|---|
| Направление подготовки | *10.05.03 "Информационная безопасность автоматизированных систем"* |
| Направленность (профиль) образовательной программы | *Обеспечение информационной безопасности распределенных информационных систем* |
| Квалификация выпускника | *специалист по защите информации* |
| Год начала подготовки *(по учебному плану)* | *2020* |
| Форма обучения | *очная* |
| Технология обучения | *традиционная* |

| Курс | Семестр | Трудоемкость, з.е. |
|---|---|---|
| *5* | *9* | *3* |

| Вид промежуточной аттестации | Обеспечивающее подразделение |
|---|---|
| *Экзамен* | *Кафедра ИБАС - Информационная безопасность автоматизированных систем* |

[1] В данном приложении представлены типовые оценочные средства. Полный комплект оценочных средств, включающий все варианты заданий (тестов, контрольных работ и др.), предлагаемых обучающемуся, хранится на кафедре в бумажном и электронном виде.

## 1 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами образовательной программы

Таблица 1 – Компетенции и планируемые результаты обучения по дисциплине

| Код и наименование компетенции | Планируемые результаты обучения по дисциплине | | |
|---|---|---|---|
| | Перечень знаний | Перечень умений | Перечень навыков |
| Профессиональные | | | |
| **ПК-23** способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа | **ПК-23.1** Знает способы формирования комплекса мер (правила, процедуры, методы) для защиты информации ограниченного доступа | **ПК-23.2** Умеет выбрать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа | **ПК-23.3** Владеет навыками контроля мер (правил, процедуры методов) для защиты информации ограниченного доступа |

Таблица 2 – Паспорт фонда оценочных средств

| **Контролируемые разделы (темы) дисциплины** | **Код контролируемой компетенции** | **Наименование оценочного средства** | **Показатели оценки** |
|---|---|---|---|
| Терминология распределенных реестров | ПК-23 | Лабораторная работа 1 | Умение выбрать способ контроля безотказного функционирования технических средств защиты информации банковской сферы |
| Исследование функции обмена файлам имежду одноранговыми устройствами | ПК-23 | Лабораторная работа 2 | Умение проводить анализ структурных и функциональных схем защищенных автоматизированных информационных систем |
| Исследование обмена файлами по сетям p2p | ПК-23 | Лабораторная работа 3 | Умение проводить анализ структурных и функциональных схем защищенных автоматизированных информационных систем |

| | | | |
|---|---|---|---|
| Исследование протоколов взаимодействия распределённых реестров | ПК-23 | Расчетно-графическая работа | Умение выбрать способ контроля безотказного функционирования технических средств защиты информации банковской сферы<br>Умение проводить анализ структурных и функциональных схем защищенных автоматизированных информационных систем |

## 2 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие процесс формирования компетенций

Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, представлены в виде технологической карты дисциплины (таблица 3).

Таблица 3 – Технологическая карта

| | Наименование оценочного средства | Сроки выполнения | Шкала оценивания | Критерии оценивания |
|---|---|---|---|---|
| 9 семестр<br>Промежуточная аттестация в форме зачета с оценкой | | | | |
| 1 | Лабораторная работа 1 | В течение семестра | 10 баллов | 10 баллов - студент правильно выполнил задание. Показал отличные знания, навыки и умения рамках освоенного учебного материала.<br>5 балла - студент выполнил задание с небольшими неточностями. Показал хорошие знания, навыки и умения рамках освоенного учебного материала.<br>3 балла - студент выполнил задание с существенными неточностями. Показал удовлетворительные знания, навыки и умения рамках освоенного учебного материала.<br>2 балла - при выполнении задания студент продемонстрировал недостаточный уровень знаний.<br>0 баллов – задание не выполнено. |
| 2 | Лабораторная работа 2 | В течение семестра | 10 баллов | 10 баллов - студент правильно выполнил задание. Показал отличные знания, навыки и умения рамках освоенного учебного материала.<br>5 балла - студент выполнил задание с небольшими неточностями. Показал хорошие знания, навыки и умения рамках освоенного учебного материала. |

| | Наименование оценочного средства | Сроки выполнения | Шкала оценивания | Критерии оценивания |
|---|---|---|---|---|
| | | | | 3 балла - студент выполнил задание с существенными неточностями. Показал удовлетворительные знания, навыки и умения рамках освоенного учебного материала.<br>2 балла - при выполнении задания студент продемонстрировал недостаточный уровень знаний.<br>0 баллов – задание не выполнено. |
| 3 | Лабораторная работа 3 | В течение семестра | 10 баллов | 10 баллов - студент правильно выполнил задание. Показал отличные знания, навыки и умения рамках освоенного учебного материала.<br>5 балла - студент выполнил задание с небольшими неточностями. Показал хорошие знания, навыки и умения рамках освоенного учебного материала.<br>3 балла - студент выполнил задание с существенными неточностями. Показал удовлетворительные знания, навыки и умения рамках освоенного учебного материала.<br>2 балла - при выполнении задания студент продемонстрировал недостаточный уровень знаний.<br>0 баллов – задание не выполнено. |
| 4 | Расчетно-графическая работа | В течение семестра | 15 баллов | 15 баллов - студент правильно выполнил задания. Показал отличные владения навыками применения полученных знаний и умений при решении профессиональных задач в рамках усвоенного учебного материала. Ответил на все дополнительные вопросы на защите.<br>10 баллов - студент выполнил задание с небольшими неточностями. Показал хорошие владения навыками применения полученных знаний и умений при решении профессиональных задач в рамках усвоенного учебного материала. Ответил на большинство дополнительных вопросов на защите.<br>5 баллов - студент выполнил задания с существенными неточностями. Показал удовлетворительное владение навыками применения полученных знаний и умений при решении профессиональных задач в рамках усвоенного учебного материала. При ответах на дополнительные вопросы на защите было допущено много неточностей.<br>0 баллов - при выполнении задания студент продемонстрировал недостаточный уровень владения навыками применения полученных знаний и умений при решении |

| | Наименование оценочного средства | Сроки выполнения | Шкала оценивания | Критерии оценивания |
|---|---|---|---|---|
| | | | | профессиональных задач в рамках усвоенного учебного материала. При ответах на дополнительные вопросы на защите было допущено множество неточностей. |
| ИТОГО: | | | 45 баллов | |
| Критерии оценки результатов обучения по дисциплине:<br>0 – 64 % от максимально возможной суммы баллов – «неудовлетворительно» (недостаточный уровень для промежуточной аттестации по дисциплине);<br>65 – 74 % от максимально возможной суммы баллов – «удовлетворительно» (пороговый (минимальный) уровень);<br>75 – 84 % от максимально возможной суммы баллов – «хорошо» (средний уровень);<br>85 – 100 % от максимально возможной суммы баллов – «отлично» (высокий (максимальный) уровень). | | | | |

## 3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие процесс формирования компетенций в ходе освоения образовательной программы

**Контрольные вопросы:**

1. Как убедиться в том, что файлы, загружаемые из сети p2p, не защищены авторским правом и не содержат вредоносное программное обеспечение?
2. Как убедиться в том, что файлы, загружаемые из одноранговой сети, не защищены авторским правоми не содержат вредоносное ПО?
3. Инструмент построения распределенной сети хранения информации, предоставляющий ряд гарантий в условиях взаимногонедоверия участников.
4. Строка символов (битовая строка), используемаякриптографическим алгоритмом при шифровании и дешифровании сообщений, постановке и проверке цифровой подписи, а также идентификации.
5. Имущество в электронной форме, созданное с использованием шифровальных (криптографических) средств.
6. Технология, позволяющая проводить обмен информацией (транзакциями) между узлами в сети без предварительной записи в блокчейн.
7. Деятельность по валидации транзакций на блокчейне.
8. Одноранговая цифровая денежная система, построенная на криптографических алгоритмах
9. Криптографический хэш открытого ключа.
10. Децентрализованное взаимодействие между двумя и более сторонами в сети
11. Технология, позволяющая увеличить степень анонимности криптовалютных транзакций.
12. Особенность протокола Bitcoin, которая позволяет нодам заверять транзакцию без загрузки полной цепочки блоков.
13. Платформа, основанная на открытом коде, где разработчики создают и запускают децентрализованные приложения, которые повышают ценность экосистемы Ethereum.

## Лист регистрации изменений к РПД

| | Номер протокола заседания кафедры, дата утверждения изменения | Количество страниц изменения | Подпись разработчика РПД |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |