


КОНКУРСНОЕ ЗАДАНИЕ  
КОМПЕТЕНЦИИ  
«РАЗРАБОТКА РЕШЕНИЙ С  
ИСПОЛЬЗОВАНИЕМ БЛОКЧЕЙН  
ТЕХНОЛОГИЙ»

2023 г.

Сотисово,  
директор филиала  
Федерального государственного  
учреждения «Федеральный центр  
информационных технологий  
и связи» Министерства  
цифрового развития  
России  
И.И. Сотисово



Конкурсное задание разработано экспертным сообществом и утверждено Менеджером компетенции, в котором установлены нижеследующие правила и необходимые требования владения профессиональными навыками для участия в соревнованиях по профессиональному мастерству.

**Конкурсное задание включает в себя следующие разделы:**

1. ОСНОВНЫЕ ТРЕБОВАНИЯ КОМПЕТЕНЦИИ.....	2
1.1. ОБЩИЕ СВЕДЕНИЯ О ТРЕБОВАНИЯХ КОМПЕТЕНЦИИ .....	2
1.2. ПЕРЕЧЕНЬ ПРОФЕССИОНАЛЬНЫХ ЗАДАЧ СПЕЦИАЛИСТА ПО КОМПЕТЕНЦИИ «РАЗРАБОТКА РЕШЕНИЙ С ИСПОЛЬЗОВАНИЕМ БЛОКЧЕЙН ТЕХНОЛОГИЙ» .....	2
1.3. ТРЕБОВАНИЯ К СХЕМЕ ОЦЕНКИ .....	5
1.4. СПЕЦИФИКАЦИЯ ОЦЕНКИ КОМПЕТЕНЦИИ.....	5
1.5.2. Структура модулей конкурсного задания (инвариант/вариатив) .....	7
2. СПЕЦИАЛЬНЫЕ ПРАВИЛА КОМПЕТЕНЦИИ.....	16
2.1. Личный инструмент конкурсанта.....	19
3. Приложения .....	20

# 1. ОСНОВНЫЕ ТРЕБОВАНИЯ КОМПЕТЕНЦИИ

## 1.1. ОБЩИЕ СВЕДЕНИЯ О ТРЕБОВАНИЯХ КОМПЕТЕНЦИИ

Требования компетенции «Разработка решений с использованием блокчейн технологий» (возрастная категория 14-16 лет) определяют знания, умения, навыки и трудовые функции, которые лежат в основе наиболее актуальных требований работодателей отрасли.

Целью соревнований по компетенции является демонстрация лучших практик и высокого уровня выполнения работы по соответствующей рабочей специальности или профессии.

Требования компетенции являются руководством для подготовки конкурентоспособных, высококвалифицированных специалистов / рабочих и участия их в конкурсах профессионального мастерства.

В соревнованиях по компетенции проверка знаний, умений, навыков и трудовых функций осуществляется посредством оценки выполнения практической работы.

Требования компетенции разделены на четкие разделы с номерами и заголовками, каждому разделу назначен процент относительной важности, сумма которых составляет 100.

## 1.2. ПЕРЕЧЕНЬ ПРОФЕССИОНАЛЬНЫХ ЗАДАЧ СПЕЦИАЛИСТА ПО КОМПЕТЕНЦИИ «РАЗРАБОТКА РЕШЕНИЙ С ИСПОЛЬЗОВАНИЕМ БЛОКЧЕЙН ТЕХНОЛОГИЙ»

*Перечень видов профессиональной деятельности, умений и знаний и профессиональных трудовых функций специалиста (из ФГОС/ПС/ЕТКС..) и базируется на требованиях современного рынка труда к данному специалисту*

Таблица №1

### Перечень профессиональных задач специалиста

№ п/п	Раздел	Важность в %
1	<b>Организация работы</b>	10
	Специалист должен знать и понимать: - Документацию и правила по охране труда и технике безопасности; - Основные принципы безопасной работы с ПК; - Значимость планирования всего рабочего процесса, как выстраивать эффективную работу и распределять рабочее время.	
	Специалист должен уметь: - Выполнять требования по охране труда и технике безопасности; - Выполнять требования техники безопасности при работе с ПК;	

	<ul style="list-style-type: none"> <li>- Идентифицировать и использовать средства индивидуальной защиты;</li> <li>- Организовывать рабочее место для максимально эффективной работы;</li> <li>- Эффективно использовать рабочее время;</li> <li>- Работать эффективно, постоянно отслеживая результаты работы;</li> <li>- Внедрять и постоянно использовать высокие стандарты качества работ и технологий.</li> </ul>	
2	<p><b>Коммуникативные и межличностные навыки общения</b></p> <p>Специалист должен знать и понимать:</p> <ul style="list-style-type: none"> <li>- Важность поддержания знаний на высоком уровне;</li> <li>- Основные требования к смежным профессиям;</li> <li>- Значение построения продуктивных рабочих отношений;</li> <li>- Важность умения решать конфликтные ситуации и недопонимания.</li> </ul>	5
	<p>Специалист должен уметь:</p> <ul style="list-style-type: none"> <li>- Формулировать задание по требованиям к продукту;</li> <li>- Консультировать и рекомендовать продукцию или решения по новым технологиям;</li> <li>- Опрашивать заказчика точно и детально для понимания требований;</li> <li>- Давать ясные инструкции по эксплуатации;</li> <li>- Подготовить письменные отчеты о проделанной работе;</li> <li>- Производить оценку стоимости и необходимого времени для выполнения задания;</li> <li>- Адаптироваться к изменениям в смежных профессиях.</li> </ul>	
3	<p><b>Программирование узла блокчейн</b></p> <p>Специалист должен знать и понимать:</p> <ul style="list-style-type: none"> <li>- Сферы и назначение блокчейн-технологии;</li> <li>- Принципы работы блокчейн-технологии;</li> <li>- Формирование транзакций;</li> <li>- Формирование блоков. Механизмы консенсусов;</li> <li>- Передача блоков;</li> <li>- Возникновение ответвлений (форков) и механизмы определения основной цепочки;</li> <li>- Симметричные и асимметричные алгоритмы шифрования;</li> <li>- Как работают сетевые протоколы (tcp/ip);</li> <li>- Создание и работа peer-to-peer сети;</li> <li>- Существующие решения на рынке: EOS, Ethereum, Bitcoin, HyperLedger, Solana, TON, Polkadot, Waves.</li> </ul>	45
	<p>Специалист должен уметь:</p> <ul style="list-style-type: none"> <li>- Правильно выбирать и применять технологию;</li> <li>- Правильно выбирать и применять шаблоны и алгоритмы при разработке;</li> <li>- Программировать на одном из языков высокого уровня, такие как Python, Go, C++, Java, JavaScript, C# и т.п.;</li> <li>- Работать со средами разработки (IDE);</li> <li>- Использовать принципы Объектно-Ориентированного Программирования (ООП) или Функционального Программирования (ФП);</li> <li>- Читать и понимать существующий код;</li> </ul>	

	<ul style="list-style-type: none"> <li>- Покрытие кода программы тестами;</li> <li>- Тестировать, отлаживать и оптимизировать код программы.</li> </ul>	
4	<p><b>Программирование умных контрактов</b></p> <p>Специалист должен знать и понимать:</p> <ul style="list-style-type: none"> <li>- Принципы работы умных контрактов в виртуальной среде;</li> <li>- Принципы создания умного контракта;</li> <li>- Принципы тестирования контракта;</li> <li>- Механизмы доставки контракта в среду выполнения;</li> <li>- Ограничения умных контрактов;</li> <li>- Взаимодействие умных контрактов;</li> <li>- Частые ошибки и уязвимости при создании умных контрактов.</li> </ul>	20
	<p>Специалист должен уметь:</p> <ul style="list-style-type: none"> <li>- Создавать умные контракты для определенной виртуальной среды;</li> <li>- Понимание ограничений на программный код, которые накладывает VM;</li> <li>- Тестирование умных контрактов;</li> <li>- Деплой умных контрактов;</li> <li>- Знание одного из языков программирования для написания контрактов.</li> </ul>	
5	<p><b>Программирование интерфейса</b></p> <p>Специалист должен знать и понимать:</p> <ul style="list-style-type: none"> <li>- Принципы создания удобного и функционального интерфейса;</li> <li>- Принципы взаимодействия со сторонним ПО.</li> </ul>	5
	<p>Специалист должен уметь:</p> <ul style="list-style-type: none"> <li>- Применять навыки системной аналитики для создания внешнего вида интерфейса;</li> <li>- Применять навыки программирования для создания интерфейса;</li> <li>- Настроить взаимодействие смарт-контракта с внешней средой.</li> </ul>	
6	<p><b>Информационная безопасность</b></p> <p>Специалист должен знать и понимать:</p> <ul style="list-style-type: none"> <li>- Современные протоколы аутентификации с использованием асимметричной криптографии;</li> <li>- Протоколы распределения асимметричных ключей в открытых системах;</li> <li>- Специфику передаваемых данных в открытой информационной системе;</li> <li>- Типовые уязвимости смарт контрактов</li> </ul>	15
	<p>Специалист должен уметь:</p> <ul style="list-style-type: none"> <li>- Применять навыки информационной безопасности для создания надежной системы аутентификации;</li> <li>- Учитывать характер данных, передаваемых в транзакциях.</li> </ul>	

### 1.3. ТРЕБОВАНИЯ К СХЕМЕ ОЦЕНКИ

Сумма баллов, присуждаемых по каждому аспекту, должна попадать в диапазон баллов, определенных для каждого раздела компетенции, обозначенных в требованиях и указанных в таблице №2.

Таблица №2

#### Матрица пересчета требований компетенции в критерии оценки

Критерий/Модуль						Итого баллов за раздел ТРЕБОВАНИЙ КОМПЕТЕНЦИИ
Разделы ТРЕБОВАНИЙ КОМПЕТЕНЦИИ И		<b>А</b>	<b>Б</b>	<b>В</b>	<b>Г</b>	
	<b>1</b>	2	3	2	3	10
	<b>2</b>	–	–	5	–	5
	<b>3</b>	25	14	2	4	45
	<b>4</b>	–	–	–	20	20
	<b>5</b>	–	–	5	–	5
	<b>6</b>	–	6	2	7	15
<b>Итого баллов за критерий/модуль</b>		27	23	16	34	<b>100</b>

### 1.4. СПЕЦИФИКАЦИЯ ОЦЕНКИ КОМПЕТЕНЦИИ

Оценка Конкурсного задания будет основываться на критериях, указанных в таблице №3:

Таблица №3

#### Оценка конкурсного задания

Критерий		Методика проверки навыков в критерии
<b>А</b>	Работа с блокчейн цепью	Оценка производится путем сравнения представленных решений с ключами-ответами, подготовленными разработчиками задания.
<b>Б</b>	Механизмы блокчейн	Оценка производится путем сравнения представленных решений с ключами-ответами, подготовленными разработчиками задания.
<b>В</b>	Презентация решения	Осуществляется оценка только представленной в докладе информации. Разрешены уточняющие вопросы, позволяющие оценить корректность и понимание Конкурсантами представленной информации. Тезисы, озвученные вне основного времени, не оцениваются.
<b>Г</b>	Аналитика	Оценка производится путем сравнения представленных решений с ключами-ответами, подготовленными разработчиками задания.

## **1.5. КОНКУРСНОЕ ЗАДАНИЕ**

Возрастной ценз: 14 лет и более

Общая продолжительность Конкурсного задания<sup>1</sup>: 10 ч.

Количество конкурсных дней: 3 дня

Вне зависимости от количества модулей, КЗ должно включать оценку по каждому из разделов требований компетенции.

Оценка знаний участника должна проводиться через практическое выполнение Конкурсного задания. В дополнение могут учитываться требования работодателей для проверки теоретических знаний / оценки квалификации.

Текст и приложения Конкурсного задания выдается участникам своевременно – в день проведения модуля или в начале каждой сессии (если модуль разделен на сессии) с предоставлением Конкурсанту времени на ознакомление с выданной частью Конкурсного задания.

### **1.5.1. Разработка/выбор конкурсного задания**

Конкурсное задание состоит из 4 модулей, включает обязательную к выполнению часть (инвариант) – 3 модуля, и вариативную часть – 1 модуль. Общее количество баллов конкурсного задания составляет 100.

Обязательная к выполнению часть (инвариант) выполняется всеми регионами без исключения на всех уровнях чемпионатов.

Количество модулей из вариативной части, выбирается регионом самостоятельно в зависимости от материальных возможностей площадки соревнований и потребностей работодателей региона в соответствующих специалистах. В случае если ни один из модулей вариативной части не подходит под запрос работодателя конкретного региона, то вариативный(е) модуль(и) формируется регионом самостоятельно под запрос работодателя. При этом время на выполнение модуля(ей) и количество баллов в критериях оценки по аспектам не меняются.

Матрица конкурсного задания доступна по ссылке <https://disk.yandex.ru/d/py2YXtBCvj4kDg>

---

<sup>1</sup> Указывается суммарное время на выполнение всех модулей КЗ одним конкурсантом.

## 1.5.2. Структура модулей конкурсного задания (инвариант/вариатив)

### Модуль А. Работа с блокчейн цепью (инвариант)

Время на выполнение модуля: 2 часа

*Проводится с полным ограничением доступа к сети Интернет.*

#### Задание 1 — Слишком много вопросов:

Используйте приложение №7 «Задание А.rar».

В директории «Задание Б» приведены файлы. Каждый файл хранит информацию о блоке в цепочке. Название файла - хэш блока, который в нем хранится.

Структура блока приведена ниже:

```
{
  "index": - индекс блока,
  "pre_hash": хэш предыдущего блока,
  "timestamp": время создания блока в формате UNIX-time,
  "transactions": [
    {
      "from": " __",
      "to": " __",
      "value": __
    } ] - список транзакций, с указанием получателя, отправителя средств и
суммы перевода,
  "secret_info": дополнительная информация в блоке,
  "nonce": nonce, добавленный в блок согласно протоколу консенсуса PoW,
  "hash": - хэш блока
}
```

Помимо основных блоков цепочки в каталоге хранятся блоки из отброшенных форков. Форком считается разбиение цепочки на две начиная с какого-то блока. Короткий форк отбрасывается и не является частью основного блокчейна.

#### Вопрос 1.

Укажите автора и номер блока, хэш которого имеет вид 0x000.....000

#### Вопрос 2.

Укажите длину наименьшего форка в системе.



**Вопрос 3.**

Укажите номер первого блока в форке наименьшей длины.

**Вопрос 4.**

Укажите длину наибольшего форка.

**Вопрос 5.**

Укажите хэш последнего блока в отброшенной ветке форка наибольшей длины.

**Вопрос 6.**

Найдите количество форков, произошедших в системе.

**Вопрос 7.**

Укажите размер вознаграждения за создание блока #71.

**Вопрос 8.**

Определите период сокращения размера вознаграждения за создание блока (каждые  $n$  блоков).

**Вопрос 9.**

Определите коэффициент сокращения вознаграждения за выработку блока. (Округлить до сотых)

**Вопрос 10.**

Определите # блока, в котором в будущем размер вознаграждения впервые окажется равен 0,09

**Вопрос 11.**

Укажите блоки, в которых в поле `secret_info` встречается дополнительная информация, блоки откинутых форков не учитываются.

**Вопрос 12.**

Соберите полученную информацию в порядке ее появления в цепочке, укажите полученное значение.

**Вопрос 13.**

Полученное ранее значение является шестнадцатеричной формой представления ключевой строки. Строка имеет следующий формат: `WSflag{_____}`

**ВНИМАНИЕ!!!!** В центре рабочего стола необходимо создать папку «2023\_A\_X», где X – номер рабочего места. Все файлы, созданные в результате выполнения решения, должны быть помещены в эту папку.

## Модуль Б. Механизмы блокчейн (инвариант)

Время на выполнение модуля: 2 часа

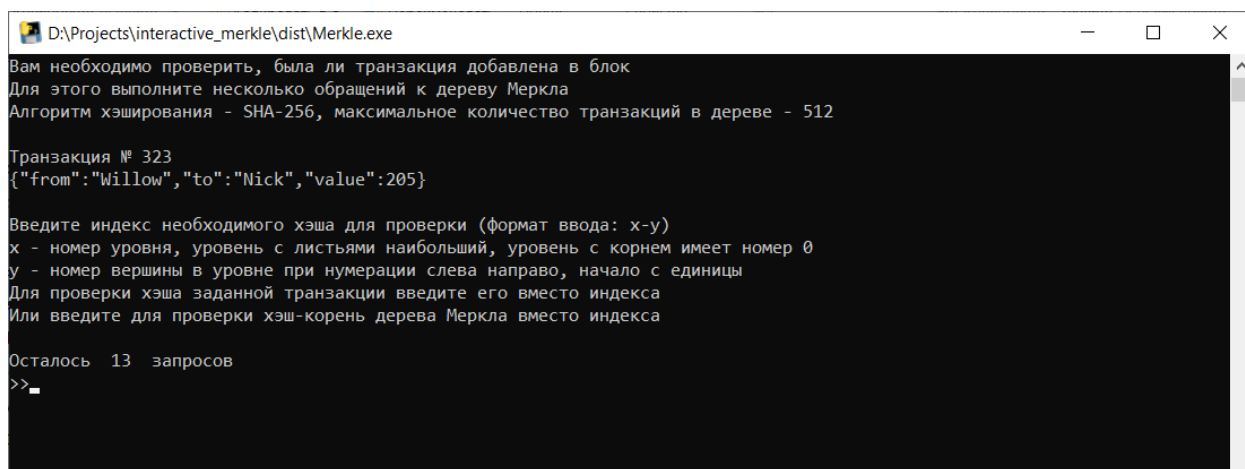
**Сессия Б1** – 1 час 30 минут. Проводится с полным ограничением доступа к сети Интернет.

### Задание 1 – Дерево Меркла 13R:

Используйте приложение №8 Merkle.exe.

Чтобы проверить, является ли транзакция частью блока используется структура, называемая деревом Меркла. Зная свою транзакцию и ее хэш можно лишь за несколько действий сделать необходимый вывод.

Конкурсант имеет на рабочем столе файл Merkle.exe. Запустив его, он получает сгенерированную транзакцию – одну из всех транзакций блока. Конкурсант имеет возможность сделать ограниченное количество запросов к системе – указать уровень и номер вершины в нем. Ответом на запрос является хэш значение этой вершины в дереве.



```
D:\Projects\interactive_merkle\dist\Merkle.exe
Вам необходимо проверить, была ли транзакция добавлена в блок
Для этого выполните несколько обращений к дереву Меркла
Алгоритм хэширования - SHA-256, максимальное количество транзакций в дереве - 512

Транзакция № 323
{"from": "Willow", "to": "Nick", "value": 205}

Введите индекс необходимого хэша для проверки (формат ввода: x-y)
x - номер уровня, уровень с листьями наибольший, уровень с корнем имеет номер 0
y - номер вершины в уровне при нумерации слева направо, начало с единицы
Для проверки хэша заданной транзакции введите его вместо индекса
Или введите для проверки хэш-корень дерева Меркла вместо индекса

Осталось 13 запросов
>>_
```

Конкурсанту необходимо вычислить хэш первой транзакции и получить корень дерева, совершив минимальное количество запросов.

Привести следующие результаты:

- кодовое слово, получаемое при нахождении верного хэша транзакции
- кодовое слово, получаемое при нахождении верного корня дерева
- скриншот с кодовым словом, получаемым при нахождении верного корня дерева, содержащий информацию об оставшемся количестве попыток.

## Задание 2 – Атака 51%

В блокчейн системе OlympiCoin, работающей на основе механизма консенсуса PoW, зарегистрировано 100 пользователей. Среднее время выработки блока составляет 5 минут 30 секунд. Один из участников решил нарушить работу сети, изменив цепочку начиная с четвертого блока. Злоумышленник смог склонить на свою сторону еще 50 человек. Узнав об угрозе целостности данных, 20 человек решили объединиться и попытаться противостоять атаке.

Считать, что атака на сеть и противодействие ей начались одновременно, сеть в этот момент просуществовала в течение 3 дней 14 минут.

Считать, что вычислительная мощность всех участников равна, а для принятия всеми участниками новой цепочки, она должна превосходить старую на 8 блоков.

Если злоумышленнику удастся нарушить работу сети, в качестве ответа укажите номер последнего блока в новой общей цепочке. В случае успешной защиты сети в качестве ответа укажите 0.

Привести следующие результаты:

- соотношение сил (правильная дробь, округлить до сотых)
- какое количество блоков было в сети к моменту начала атаки
- какое преимущество (количество блоков) было у защитников к началу атаки
- на каком номере блока злоумышленники успешно завершат атаку
- сколько блоков останутся не поврежденными
- какое время понадобится злоумышленникам для совершения атаки, округлить до минут

**ВНИМАНИЕ!!!!** В центре рабочего стола необходимо создать папку «2023\_Б1\_X», где X – номер рабочего места. Все файлы, созданные в результате выполнения решения, должны быть помещены в эту папку.

*Сессия Б2 – 30 минут.*

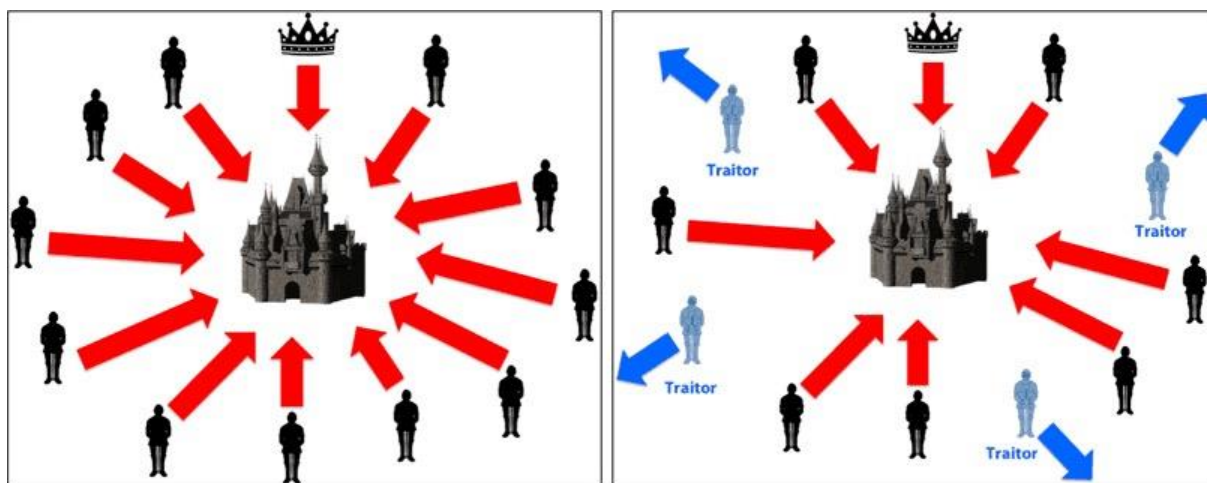
*Выполняется с доступом к сети Интернет, при этом использование социальных сетей, мессенджеров, почтовых сервисов и иных ресурсов, которые могут содержать личные ресурсы и файлы конкурсантов, строго запрещено!*

### **Задание 3 - Полководцы не договорятся**

Представьте себе средневековье, каменный замок в окружении врагов. Ночь перед великим сражением с противником. Атакующая армия состоит из N легионов, каждым из которых командует свой полководец. Полководцы подчиняются единственному главнокомандующему.

В то же самое время войска истощены, измотаны и находятся в упадке, что привело к возможному появлению предателей в лице полководцев и главнокомандующего, но остались и верные бойцы.

Ночью главнокомандующий отдает приказ, который распространяется на всех полководцев. В приказе указано, как надлежит поступить на рассвете (про атаку на рассвете всем известно заранее, визуально все полководцы видят рассвет). Сообщение приказа простое - «атаковать» или «отступать».



Скоординированная атака, ведущая к победе

Несогласованная атака, ведущая к поражению

#### **Возможные исходы:**

1. При отступлении всех верных полководцев - замок сохранится, и армия не потеряет солдат (промежуточный исход);
2. При нападении всех верных полководцев - замок будет захвачен, а противник - уничтожен (благоприятный исход);

3. Если часть верных полководцев пойдет в атаку, а остальные - отступят, то противник постепенно, со временем, сможет уничтожить всю армию главнокомандующего (неблагоприятный исход)

В случае, если главнокомандующий окажется предателем, то следует учитывать его возможность отдачи разным полководцам противоположных указаний, чтобы собственноручно развалить армию. Поэтому, полководцы должны учитывать данные обстоятельства для недопущения несогласованных действий.

При решении полководца действовать независимо от других и не взирая на приказы сверху (сделать случайный выбор), вероятность положительного исхода крайне низкая. Поэтому, полководцы нуждаются в обмене информации между друг другом, чтобы принять единое решение.

#### **Уточнение задачи.**

$N$  полководцев готовятся к атаке. Для координации действий они применяют надежный канал связи, любая подмена сказанного исключена, например ключевые фразы, которые были выработаны заранее до появления “внештатных” ситуаций.

При этом  $M$  полководцев, очевидно, являются предателями и активно пытаются разрушить единомыслие всех остальных. Суть соглашения в том, чтобы каждый полководец обладал истинной информацией о количестве всех участвующих полководцах и их войск, и чтобы все полководцы приняли единое решение (пусть и с промежуточным исходом) относительно нападения или отступления на крепость.

Задание:

1. Узнать, о какой известной теореме идет речь
2. Пояснить, как данная теорема применима к технологии блокчейн
3. Решить задачу при условиях  $N = 3, M = 2$
4. Решить задачу при условиях  $N = 4, M = 1$

**ВНИМАНИЕ!!!!** В центре рабочего стола необходимо создать папку «2023\_Б2\_Х», где Х – номер рабочего места. Все файлы, созданные в результате выполнения решения, должны быть помещены в эту папку.

## Модуль В. Презентация (инвариант)

Время на выполнение модуля: 2 часа

*Выполняется с доступом к сети Интернет, при этом использование социальных сетей, мессенджеров, почтовых сервисов и иных ресурсов, которые могут содержать личные ресурсы и файлы конкурсантов, строго запрещено!*

### Задание:

Перед конкурсантом стоит задача спроектировать сервис для продажи NFT токенов в различных блокчейн системах, например Ethereum и BNB Chain. Вы также можете предложить собственную идею в любой отрасли.

На работу Модуля Г отводится 2 часа. Первый час времени используется для подготовки презентации блокчейн-решения. Второй час используется для заслушивания докладов участников.

В ходе презентации необходимо отобразить следующие моменты:

- ✓ техническое задание проекта;
- ✓ планирование всех задач проекта;
- ✓ архитектуру проекта: основные функциональные модули системы и их взаимосвязь;
- ✓ подробную схему работы модуля авторизации;
- ✓ обоснование использования технологии блокчейн;
- ✓ стек технологий для разработки;
- ✓ графический интерфейс решения;
- ✓ возможные уязвимости и недостатки проекта;
- ✓ план дальнейшего развития проекта;
- ✓ план коммерциализации проекта.

Регламент устного выступления: 7 минут на доклад + 3 минуты ответы на вопросы экспертов.

**ВНИМАНИЕ!!!!** В центре рабочего стола необходимо создать папку «2023\_В\_X», где X – номер рабочего места. Все файлы, созданные в результате выполнения решения, должны быть помещены в эту папку (презентация проекта).

## Модуль Г. Аналитика (вариатив)

Время на выполнение модуля: 4 часа

*Сессия Г1 – 2 часа. Выполняется с доступом к сети Интернет, при этом использование социальных сетей, мессенджеров, почтовых сервисов и иных ресурсов, которые могут содержать личные ресурсы и файлы конкурсантов, строго запрещено!*

### Задание 1 – Платите BitCoin'ом:

Используйте приложение №9 Кошелек.jpg.



Проведите расследование:

Какой компании предположительно принадлежит данный биткойн кошелек (Маска ответа – ????? ?????)?

Укажите любые дополнительные сведения, которые вы смогли узнать в ходе расследования об этом адресе и обстоятельствах, из-за которых он привлек наше внимание.

### Задание 2 – Токены:

Третьего сентября 2020 года в блокчейн сети BNB Chain был опубликован смарт контракт токена формата ERC20.

Конкурсанту необходимо указать:

- хэш транзакции публикации этого контракта;
- номер блока, содержащий эту транзакцию;
- адрес автора транзакции;
- какой организации принадлежит этот адрес;
- примерную стоимость одного токена;
- примерное количество активных токенов;
- название этого токена;
- обозначение этого токена;
- количество десятичных разрядов в исчислении токена;
- примерная капитализация всех токенов контракта;
- уберите из названия токена первое слово. Чем то, что получилось, отличается от нашего токена;
- указать на неточность в формулировке задания;
- какое примерное количество пользователей владеет тем или иным количеством токена;
- какой процент токенов принадлежит пользователю, владеющему наибольшим количеством токенов.

**ВНИМАНИЕ!!!! В центре рабочего стола необходимо создать папку «2023\_Г1\_X», где X – номер рабочего места. Все файлы, созданные в результате выполнения решения, должны быть помещены в эту папку.**



*Сессия Г2 – 2 часа. Проводится с полным ограничением доступа к сети Интернет.*

### **Задание 3 – Смарт-контракт:**

Используйте приложение №10 «Contract.sol».

Смарт-контракт был написан с использованием компилятора языка программирования Solidity версии 0.8.0. Не разрешается изменять описание и определение приведенных в контракте структур данных. Код смарт-контракта может быть размещен в открытом доступе.

Конкурсантам необходимо сформировать:

- отчет по синтаксису – указать строки, в которых допущены синтаксические ошибки и их исправление;
- отчет по функционалу – описать функционал смарт-контракта, его функций;
- отчет по логике – указать на ошибки в логике работы контракта, внести предложения по их устранению;
- отчет по проверкам – предложить текст сообщений об ошибке в существующих в контракте проверках;
- отчет по информационной безопасности – указать на существующие недостатки контракта (ошибки, уязвимости и т.д.) с точки зрения информационной безопасности.
- оптимизация смарт-контракта – указать на недостатки разработанного смарт-контракта, предложить варианты его оптимизации.

1	pragma solidity >0.5.0;
2	contract Contract{
3	
4	struct User{
5	uint balance;
6	string login;
7	}
8	mapping(string >> address) public logins;
9	mapping(address >> User) public users;
10	address root = msg.sender;
11	
12	function create_user(string memory login, string memory FIO) public{

```

13     require(logins[login] ==
0x0000000000000000000000000000000000000000000000000000000000000000, "_____");
14     login[login] = msg.sender;
15     users[msg.sender] = User(FIO, msg.sender.balance, login);
16 }
17
18 function get_balance(address user_address) public view returns(uint){
19     return(users[user_address].balance);
20 }
21
22 function send_money(address payable adr_to) public payable {
23     adr_to.transferring(msg.sender);
24 }
25
26 struct Donation{
27     uint donate_id;
28     string name;
29     address user;
30     uint amount;
31     uint deadline;
32     address[] sender;
33     uint[] value;
34     bool status;
35     string info;
36 }
37
38 Donation donation;
39
40 function ask_to_donate(string memory name, uint amount, uint deadline, string
memory info) public {
41     address[] memory sender;
42     uint value;
43     donation.push(Donation(donation.length, name, msg.sender, amount,
deadline, sender, value, false, info));
44 }
45
46 function participate(uint donation_id) public payable{
47     require(donation[donation_id].status == false, "_____");
48     require(msg.value > 0, "_____");
49     donation[donation_id].sender.push(msg.sender);
50     donation[donation_id].value.push(msg.value);
51 }
52
53 function get_donation(uint donation_id) public view returns(uint, string
memory, address, uint, uint, bool){

```

```

54     return(donation_id, donation[donation_id].name, donation[donation_id].user,
donation[donation_id].amount, donation[donation_id].deadline,
donation[donation_id].status);
55     }
56     function get_donation_2(uint donation_id) public view returns(address[]
memory, uint[] memory, string memory) {
57         return(donation[donation_id].sender, donation[donation_id].value,
donation[donation_id].data);
58     }
59
60     function get_donation_number() public view return(uint) {
61         return donation.len();
62     }
63
64     function get_total(uint donation_id) public view returns(uint){
65         uint total = 0;
66         for (uint i = 0; i < donation[donation_id].value.length; i++){
67             total = donation[donation_id].value[i];
68         }
69         return total;
70     }
71
72     function finish(uint donation_id) public{
73         require(msg.sender == donation[donation_id].user, "_____");
74         require(donation[donation_id].status == false, "_____");
75         uint total = get_total(donation_id);
76         if (total ** 2 >= donation[donation_id].amount){
77             payable(donation[donation_id].user).transfer(total);
78         }
79         else{
80             for (uint i = 0; i > donation[donation_id].value.length; i++) {
81 payable(donation[donation_id].sender[i]).transfer(donation[donation_id].value[i]);
82             }
83         }
84         donation[donation_id].status = false;
85     }
86 }

```

**ВНИМАНИЕ!!!! В центре рабочего стола необходимо создать папку «2023\_Г2\_X», где X – номер рабочего места. Все файлы, созданные в результате выполнения решения, должны быть помещены в эту папку.**

## 2. СПЕЦИАЛЬНЫЕ ПРАВИЛА КОМПЕТЕНЦИИ<sup>2</sup>

### 2.1. Личный инструмент конкурсанта

Список материалов, оборудования и инструментов, которые конкурсант может или должен привезти с собой на соревнование.

Нулевой - нельзя ничего привозить.

### 2.2. Материалы, оборудование и инструменты, запрещенные на площадке

Конкурсантам запрещено использовать мобильные устройства связи, персональные компьютеры и иную личную технику на конкурсной площадке в дни с С-1 до С3 во время нахождения на конкурсной площадке. В случае нарушения данного требования Конкурсант в первый раз получает предупреждение, в следующий раз отстраняется от выполнения текущего Модуля.

### 2.3. Дополнительно

Вопрос	Специальные правила
Сохранение решения конкурсантами	<ul style="list-style-type: none"><li>Решение должно быть сохранено в указанную в Конкурсном задании директорию, в случае нарушения инструкций решение не проверяется.</li></ul>
Временной регламент	<ul style="list-style-type: none"><li>В случае выполнения участником модуля Конкурсного задания в непредназначенное для этого время, в том числе во время выполнения другого модуля, такое решение не будет оценено.</li><li>За не прекращение выполнения Конкурсного задания по команде «СТОП» Главного эксперта или ответственных за хронометраж Экспертов в соответствии с временем выполнения Модуля или в иных ситуациях к Конкурсантам применяются штрафные санкции в виде снижения общей суммы баллов на 1 балл.</li></ul>
Технические средства – физические носители данных	<ul style="list-style-type: none"><li>Конкурсантам разрешается использовать только физические носители, предоставляемые организатором чемпионата. Запрещается использовать любые другие носители в устройствах Конкурсантов.</li><li>Нельзя выносить за пределы рабочей площадки физические носители или любые другие портативные устройства хранения данных.</li><li>Физические носители данных должны предъявляться главному эксперту в конце каждого дня для безопасного хранения, их нельзя выносить за пределы рабочей площадки.</li><li>При выявленном нарушении работа модуля не оценивается.</li></ul>
Технические средства — персональные устройства для фото- и видеосъемки	<ul style="list-style-type: none"><li>Экспертам и переводчикам разрешается использовать на рабочей площадке персональные устройства для фото- и видеосъемки, при этом запрещена фиксация информации о Конкурсном задании, критериях и ведомостях оценки, деталях выполнения задания Конкурсантами.</li></ul>

<sup>2</sup> Указываются особенности компетенции, которые относятся ко всем возрастным категориям и чемпионатным линейкам без исключения.

Программное обеспечение	<ul style="list-style-type: none"> <li>• Конкурсанты могут создавать программные продукты, оформлять инструкции или делать заметки, находясь на рабочей площадке, однако их никогда нельзя забирать с рабочей площадки.</li> <li>• За использование материалов, файлов, подготовленных вне конкурсного времени и за пределами конкурсной площадки, в том числе шпаргалок, материалов полученных в сети Интернет (если иное не указано в Конкурсном задании), выполняемый модуль Конкурсного задания не оценивается.</li> </ul>
Отказ оборудования	<ul style="list-style-type: none"> <li>• Если имеется явное доказательство того, что конкурсанты сами причинили ущерб оборудованию, им не будет предоставляться замена и дополнительное время.</li> </ul>
Контроль за конкурсантами	<ul style="list-style-type: none"> <li>• Конкурсантов необходимо постоянно контролировать во время их работы. Эксперты, в чьи обязанности входит контроль, должны принять меры для того, чтобы их заменил другой эксперт, если им необходимо уйти.</li> <li>• Экспертам не разрешается контролировать своего конкурсанта-компатриота.</li> </ul>
Поведение конкурсантов	<ul style="list-style-type: none"> <li>• За использование ненормативной лексики устно во время выполнения Конкурсного задания или во время защиты своих работ, а также письменно в представленных к проверке файлах к Конкурсанту применяются штрафные санкции в виде снижения общей суммы баллов на 5 баллов.</li> <li>• Общение участников во время выполнения Конкурсного задания запрещено, в случае неоднократного нарушения запрета участники дисквалифицируются на оставшееся время конкурсного дня.</li> </ul>

### 3. Приложения

Приложения

Приложение №1 [Инструкция по заполнению матрицы конкурсного задания](#)

Приложение №2 [Матрица конкурсного задания](#)

Приложение №3 [Критерии оценки](#)

Приложение №4 [Инструкция по охране труда и технике безопасности по компетенции «Разработка решений с использованием блокчейн технологий».](#)