Программа учебной дисциплины «Финансовые технологии»

Утверждена
Академическим советом ООП
Протокол № 2.03-09/2706-01 от «27» июня 2018г.

Автор	Запечников Сергей Владимирович, SVZapechnikov@mephi.ru
Число кредитов	6
Контактная работа (час.)	58
Самостоятельная работа (час.)	170
Курс	1
Формат изучения дисциплины	без использования онлайн курса

1 Цели освоения дисциплины

Целями освоения дисциплины «Финансовые технологии» являются:

- Ознакомление студентов с практиками применения финансовых технологий в бизнесе;
- Формирование у студентов представления о бизнес-моделях и бизнес-кейсах, исходя их опыта приглашенных специалистов;
- Развитие у студентов навыков межличностного общения с профессионалами из области финансовых технологий, приобретение контактов с представителями из бизнеса.

Настоящая дисциплина относится к циклу дисциплин о технологиях, которые драматически меняют современные бизнес-модели финансовых организаций.

Для освоения учебной дисциплины студенты должны владеть знаниями и компетенциями по макроэкономике, которая является адаптационной дисциплиной.

Основные положения дисциплины должны быть использованы в дальнейшем при изучении дисциплин:

- Разработка смарт-контрактов и приложений для распределенных реестров.

2 Формы контроля знаний студентов

Тип контроля	Форма контроля	1 год				Параметры
		1	2	3	4	
Промежуточный	Домашнее задание 1		*			Письменный
	Домашнее задание 2					Письменный
	Контрольная работа 1		*			Тестовые задания
	Контрольная работа 2			*		Письменный
	Защита проекта				*	Защита проекта

Итоговый	Отсутствует					

3 Критерии оценки знаний, навыков

В курсе предусмотрено несколько форм контроля знания:

- Выполнение домашних заданий
- Контрольные работы и тестирования
- Защите проекта, формирующая навыки работы в команде, понимание ландшафта применения финансовых технологий и выявление основных тенденций в сфере.

Оценки по всем формам контроля выставляются по 10-ти балльной шкале.

4 Порядок формирования оценок по дисциплине

Результирующая оценка по дисциплине рассчитывается по формуле

$$О\_итог = 0.15 \times О\_дз1 + 0.25 \times О\_кр1 + 0.15 \times О\_дз2 + 0.25 \times О\_кр2 + 0.2\ О\_проект$$

Оценка за проект выставляется комиссией, состоящей из преподавателей ВШЭ и представителей бизнеса, после защиты проекта.

Тематический план модуля «Блокчейн-технологии - 1» в рамках курса «Финансовые технологии»

Тема 1. Введение в блокчейн-технологии (4 часа). Основные идеи, лежащие в основе блокчейн-технологий: децентрализация, распределенный реестр, цепочка блоков, достижение консенсуса. Краткий очерк истории развития блокчейн-технологий.

Техническая реализация систем распределенного реестра: транспортный уровень, уровень хранения данных, прикладной уровень. Одноранговые (пиринтовые) сети как основа транспортного уровня. Понятие ноды. Взаимодействие клиентов с нодами. Сетевая структура БД (ациклический ориентированный граф) как основа уровня хранения данных. Смарт-контракты как основа прикладного уровня. Простейшие примеры смарт-контрактов.

Два типа блокчейн-платформ: открытые (permissionless) и частные (permissioned), их сравнение. Отличия открытых и частных блокчейн-платформ. Основные проблемы блокчейн-платформ: безопасность и масштабируемость.

Тема 2. Основы криптографии (6 часов). Криптография как наука о безопасности связи. Основные понятия криптографии. Симметричная и асимметричная криптография.

Основы симметричной криптографии. Шифры замены и шифры перестановки, их композиции. Классические шифры. Шифр Вернама. Совершенная секретность по Шеннону. Одноразовый шифрблокнот. Симметричное шифрование. Современные практически стойкие шифры. Блочные и поточные шифры. ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015.

Понятия однонаправленной функции, однонаправленной функции с секретом (с потайной дверью). Основные алгебраические структуры, используемые в криптографии: группы, кольца, поля. Примеры алгебраических структур, используемых в криптографии. Открытое распределение ключей. Электронная цифровая подпись (ЭЦП). Применение ЭЦП для контроля подлинности. Совместное применение ЭЦП и хэш-функции. Схема подписи RSA. Российский стандарт подписи ГОСТ Р 34.10-2012. Криптографическая хэш-функция. Свойства хэш-функции: сжатие, однонаправленность, трудность обнаружения коллизий. Применение хэш-функции для контроля целостности данных. Российский стандарт хэш-функции ГОСТ Р 34.11-2012. Функции криптографии в блокчейн-платформах.

Тема 3. Принципы функционирования блокчейн-платформ (6 часов). Хранение данных в системах распределенного реестра. Формирование блоков транзакций. Дерево Меркле. Формирование цепочки блоков. Достижение консенсуса в блокчейн-платформах открытого типа путем доказательства выполнения работы (proof-of-work), используемая при этом вычислительно сложная задача подбора значения хэш-функции. Вознаграждение нод, майнинг криптовалют. Особенности доказательства выполнения работы: регулирование сложности задачи, разрешение вилок (forks). Атака 51%.

Способы достижения консенсуса в блокчейн-платформах закрытого типа. Фундаментальные теоремы о консенсусе. «Задача о византийских генералах» и её решения для случаев подписанных и неподписанных сообщений. Протоколы византийского соглашения, их характерные особенности и пороги устойчивости к воздействию злоумышленника.

Тема 4. Сферы применения блокчейн-технологий (4 часа). Чисто реестровые приложения блокчейн-технологий: криптовалюты, доказательная регистрация событий и пр.

Блокчейн как платформа децентрализованных вычислений. Смарт-контракты. Примеры смарт-контрактов. Языки программирования смарт-контрактов. Приложения, основанные на использовании блокчейна как платформы децентрализованных вычислений: управление цепочками поставок, отслеживание происхождения товаров, электронные договоры и сделки, медицинские информационные системы. Краудсорсинговые применения.

Промежуточный контроль: Прием домашнего задания (2 часа). Контрольная работа (2 часа).

Литература:

1. Тапскотт А., Тапскотт Д. Технология блокчейн – то, что движет финансовой революцией сегодня. М.: Эксмо, 2017. 448 с.
2. Генкин А., Михеев А. Блокчейн. Как это работает и что ждет нас завтра. М.: Альпина Паблишер, 2018. 592 с.
3. Нараян П. Блокчейн. Разработка приложений. СПб.: БХВ-Петербург, 2018. 256 с.
4. Могайар У., Бутерин В. Блокчейн для бизнеса. М.: Эксмо, 2017. 224 с.
5. Блокчейн: как он работает, и почему эта технология изменит мир. URL: https://habr.com/company/iticapital/blog/340992/
6. Антонопулос А. Осваиваем биткойн. Программирование блокчейна. М.: ДМК-Пресс, 2018. 428 с.

Домашнее задание по модулю «Блокчейн-технологии – 1»:

Изучение источников в сети Интернет и составление аналитического отчета об одной из блокчейн-платформ. Рекомендуемый план аналитического отчёта о блокчейн-платформе:

1. Титульный лист: наименование дисциплины, ФИО студента, № варианта, дата сдачи отчета.
2. Справочные сведения: название, авторы (руководители проекта), состояние (стадии развития) проекта: прототип, действующая сеть, даты запуска проекта и т.п.
3. Тип платформы: permissionless, permissioned, комбинированная. Условия доступа к системе для пользователей: процедура регистрации (если permissioned), требуемое ПО и пр.
4. Консенсус: какой метод/протокол консенсуса используется (основная идея, схема и т.п.), требуется ли криптовалюта для работы механизма консенсуса, и, если да, поддержка эмиссии криптовалют (ограниченная, неограниченная, каков механизм).
5. Технические характеристики платформы: одно-/многофункциональная платформа, поддержка смарт-контрактов, поддержка языков программирования смарт-контрактов, наличие API, SDK, открыт ли исходный код проекта, поддержка стандартов на криптографические функции (хэш-функции, цифровая подпись).
6. Приложения: в какой сфере, примеры проектов/приложений на платформе (если платформа многофункциональная), степень внедрения результатов и их практическая ценность.

7. Особенности и конкурентные преимущества платформы: по оценкам разработчиков, пользователей, публикаций в интернете.

8. Перспективность и позиции платформы на рынке: Ваши выводы о новизне, креативности, ценности проекта, перспективах его использования.

9. Список использованных источников: ссылки на сайт, whitepaper, документацию.

Приложения (необязательный элемент): возможные варианты – глоссарий, статистические сведения (динамика развития, капитализация и пр.), технические схемы, спецификации протоколов и пр.

Объём отчета – не более 10 страниц, текст должен быть представлен на русском языке (не допускается вставлять англоязычные термины в русскоязычный текст – требуется предложить перевод). Формат файла – doc, docx.

Критерии оценки домашнего задания:

- полнота изложения материала, использование разных источников, отсутствие фактических ошибок;
- логичность, последовательность суждений, обоснованность выводов;
- понятность и удобочитаемость текста, грамотность изложения, отсутствие грамматических и стилистических ошибок.

Варианты заданий:

№ варианта	Название блок-чейн-платформы	Ссылка на сайт
1	Hyperledger Iroha	https://www.hyperledger.org/projects/iroha
2	Dfinity	https://dfinity.org/
3	Hyperledger Saw-tooth	https://www.hyperledger.org/projects/sawtooth
4	BigChainDB	https://www.bigchaindb.com/
5	Hyperledger Indy	https://www.hyperledger.org/projects/hyperledger-indy
6	OpenChain	https://www.openchain.org/
7	R3 Corda	http://www.corda.net/discover/technology.html
8	BitShares	https://bitshares.org/
9	Quorum	https://www.jpmorgan.com/global/Quorum
10	IOTA	https://www.iota.org/
11	Tendermint	https://tendermint.com/
12	Stellar	https://www.stellar.org/
13	Exonum	https://exonum.com/
14	Ripple XRP	https://ripple.com/
15	Kaleido	https://kaleido.io/
16	Symbiont	https://symbiont.io/
17	NEM	https://nem.io/
18	Kadena	https://kadena.io/
19	Toda-Algorand	https://www.todarand.com/
20	Chain	https://chain.com/
21	Coda	https://codaprotocol.com/
22	Cardano	https://www.cardano.org/en/home/
23	Verge	https://vergecurrency.com/
24	Zilliqa	https://zilliqa.com/
25	Monero	https://getmonero.org/
26	EOS	https://eos.io/
27	Zcash	https://z.cash/
28	ArcBlock	https://www.arcblock.io/
29	MultiChain	https://www.multichain.com/
30	Aion	https://aion.network/

Контрольная работа по модулю «Блокчейн-технологии – 1»:

Контрольная работа проводится в письменной форме. Время на выполнение работы – 2 акад.часа. Контрольная работа состоит из двух частей. Первая часть предполагает тестирование – выбор вариантов ответов на вопросы из предложенного списка. На вопрос может быть более одного варианта правильного ответа.

Образец теста:

№ п/п	Вопрос и варианты ответа		Ответ
1	Чем отличаются асимметричные криптосистемы (двухключевых, криптосистем с открытым ключом) от симметричных криптосистем (одноключевыми, криптосистемами с секретным ключом)?		
	а)	Скорость выполнения операций шифрования в асимметричных криптосистемах на несколько порядков выше, чем в симметричных	
	б)	Скорость выполнения операций шифрования в асимметричных криптосистемах на несколько порядков ниже, чем в симметричных	
	в)	Для передачи ключей от одного участника к другому в асимметричных криптосистемах не требуются защищенные каналы связи	
	г)	Электронная цифровая подпись, в отличие от симметричного блочного шифра, не может быть использована для обеспечения секретности (конфиденциальности) сообщений	

Вторая часть контрольной работы предполагает ответы на вопросы в свободной форме. **Образцы вопросов контрольной работы:**

1. Архитектура блокчейн-платформ: транспортный уровень, уровень хранения данных, прикладной уровень.
2. Принцип достижения консенсуса путем доказательства выполнения работы (proof-of-work). Свойства криптографической хэш-функции, которые используются для доказательства выполнения работы. Примеры блокчейн-платформ, в которых используется доказательство выполнения работы.
3. Принцип достижения консенсуса путем выполнения протокола византийского соглашения. Примеры блокчейн-платформ, в которых используются протоколы византийского соглашения.
4. Реестровые применения блокчейн-платформ. Пример применения блокчейн-платформы для ведения распределенного реестра транзакций.
5. Смарт-контракты. Пример применения блокчейн-платформы для учета активов с использованием смарт-контрактов.

Тематический план модуля «Блокчейн-технологии - 2» в рамках курса «Финансовые технологии»

Тема 1. Блокчейн-платформы открытого типа (6 часов). Обзор блокчейн-платформ открытого типа: Bitcoin – первая платформа для поддержки криптовалюты, Altcoins – «альтернативные» криптовалютные платформы, Ethereum – первая платформа с поддержкой смарт-контрактов.

Математическая модель системы распределенного реестра открытого типа (на примере платформы Ethereum). Типы аккаунтов на платформе Ethereum: внешние аккаунты и контракт-аккаунты. Модель хранения данных и исполняемого кода. Децентрализованная виртуальная машина Ethereum (EVM).

Тема 2. Блокчейн-платформы закрытого типа (6 часов). Платформы для систем распределенного реестра закрытого типа. Проект Hyperledger. Платформы Hyperledger Fabric, Hyperledger Sawtooth, Hyperledger Iroha, их характерные особенности и ограничения. Платформа Corda. Платформа Quorum. Платформы с поддержкой российской криптографии: «Мастерчейн», Exonum.

Математическая модель системы распределенного реестра закрытого типа (на примере платформы Hyperledger Fabric). Формат хранения данных. Архитектура платформы: ноды различных типов – endorsers, orderers, peers. Модульная архитектура платформы, возможность замены протоколов консенсуса. Трехэтапный процесс формирования новых блоков.

Гибридные платформы для систем распределенного реестра: BitcoinNG, Omniledger, Toda-Algorand.

Тема 3. Обеспечение информационной безопасности блокчейн-платформ (4 часа). Разграничение доступа к распределенному реестру на примере платформы Hyperledger Fabric: каналы, частное хранение данных, разделение функций нод, задание политики валидации транзакций. Прямые коммуникации между клиентами блокчейн-платформы: off-chain-вычисления, lightning networks.

Обеспечение конфиденциальности исполнения смарт-контрактов. Доказательства с нулевым разглашением: zk-SNARKs, zk-STARKs, Bulletproofs, range proofs и др. Проблемы их применения. Примеры криптовалют, в которых используются доказательства с нулевым разглашением: Monero, Zcash.

Тема 4. Примеры прикладных решений на основе блокчейн-платформ (4 часа).

Пример решения на основе блокчейн-платформы открытого типа – система распределения заказов на работы и поиска исполнителей.

Пример решения на основе блокчейн-платформы закрытого типа – прототип системы валовых расчетов реального времени Ubin на основе блокчейн-платформ Corda, Hyperledger Fabric и Quorum.

Текущий и итоговый контроль. Приём домашнего задания (2 часа). Контрольная работа (2 часа).

Литература:

1. Документация на платформу Ethereum: http://www.ethdocs.org/en/latest/
2. Документация на платформу Hyperledger Fabric: https://hyperledger-fabric.readthedocs.io/en/release-1.2/index.html
3. Спецификация протокола Zcash: https://github.com/zcash/zips/blob/master/protocol/protocol.pdf
4. Сайт проекта Monero: https://ww.getmonero.org/
5. Сайт проекта UBIN. URL: https://github.com/project-ubin

Текущий и итоговый контроль.

Текущий контроль по модулю «Блокчейн-технологии – 2» проводится в форме домашнего задания. Итоговый контроль – в форме контрольной работы.

Домашнее задание по модулю «Блокчейн-технологии – 2»:

Разработка учебного проекта технического задания на создание прикладной программы на базе блокчейн-платформы.

5 Содержание блока бизнес-кейсов

Помимо введения в блокчейн в рамках дисциплины (темы 1-8 из раздела Тематический план УД) разбираются бизнес-кейсы и/или бизнес-модели из практики выступающих.

Темы кейсов:

- Продукты Глобальных рынков. Алготорговля

- Вычисления на квантовом компьютере
- Искусственный интеллект. Роботехника.
- Venture Capital. Инвестирование в стартапы.
- ICO
- Кибербезопасность
- Будущее банковской сферы

Из-за наличия преподавателей, работающих в бизнес-направлениях, содержание дисциплины может меняться. Студенты будут заранее оповещены о деталях каждого мастер-класса.

Итоговый проект защищается представлением презентации команды по выбранной теме. Каждая тема для презентации освещается спикерами из бизнес-направлений, рассказывающих об истории формирования технологии и ее применении в бизнесе. Темы презентаций и распределение по командам проходит в начале 4-го модуля.

6 Учебно-методическое и информационное обеспечение дисциплины

6.1 Базовые учебники

7. Тапскотт А., Тапскотт Д. Технология блокчейн – то, что движет финансовой революцией сегодня. М.: Эксмо, 2017. 448 с.
8. Генкин А., Михеев А. Блокчейн. Как это работает и что ждет нас завтра. М.: Альпина Паблишер, 2018. 592 с.
9. Нараян П. Блокчейн. Разработка приложений. СПб.: БХВ-Петербург, 2018. 256 с.
10. Могайар У., Бутерин В. Блокчейн для бизнеса. М.: Эксмо, 2017. 224 с.
11. Блокчейн: как он работает, и почему эта технология изменит мир. URL: https://habr.com/company/iticapital/blog/340992/
12. Антонопулос А. Осваиваем биткойн. Программирование блокчейна. М.: ДМК-Пресс, 2018. 428 с.
13.

6.2 Дополнительная литература

1. Документация на платформу Ethereum: http://www.ethdocs.org/en/latest/
2. Документация на платформу Hyperledger Fabric: https://hyperledger-fabric.readthedocs.io/en/release-1.2/index.html
3. Спецификация протокола Zcash: https://github.com/zcash/zips/blob/master/protocol/protocol.pdf
4. Сайт проекта Monero: https://ww.getmonero.org/
5. Сайт проекта UBIN. URL: https://github.com/project-ubin
6. Mohri M., Rostamizadeh A., Talwalkar A. Foundations of Machine Learning. MIT Press, 2012.
7. Murphy K. Machine Learning: A Probabilistic Perspective. MIT Press, 2012.
8. Schutt R., O'Neil C. Doing data science: Straight talk from the frontline. – " O'Reilly Media, Inc.", 2013.
9. McMillan J. The end of banking: money, credit, and the digital revolution. – BookBaby, 2015.
10. John Lu Z. Q. The elements of statistical learning: data mining, inference, and prediction //Journal of the Royal Statistical Society: Series A (Statistics in Society). – 2010. – Т. 173. – №. 3. – С. 693-694.
11. Alpaydin E. Introduction to machine learning. – MIT press, 2014.
    MacKay D. J. C. Information theory, inference and learning algorithms. – Cambridge university press, 2003.
12. Witten I. H. et al. Data Mining: Practical machine learning tools and techniques. – Morgan Kaufmann, 2016.
13. Mohammed J. Zaki, Wagner Meira Jr. Data Mining and Analysis. Fundamental Concepts and Algorithms. Cambridge University Press, 2014.