**Александр Викторович Беленов, руководитель лаборатории ChainLab научного центра «Идея», архитектор блокчейн-систем (**[**https://chainlab.ru/**](https://chainlab.ru/)**)**

Направления исследований и научного руководства:

1. Любые темы, связанные с Web3,
2. Account Abstraction
3. DiD (decentralized identification)
4. DAO
5. Репутация и механизмы ее честного обеспечения
6. Прикладная токеномика

До 3-х студентов на научное руководство.

**Юрий Александрович Янович**

*Научный работник в области блокчейна с опытом, включающим машинное обучение и математическую статистику. Параллельно академической деятельности, 5 лет работал в компании Bitfury, где приложил руку к созданию фреймворка Exonum и первого применения блокчейна на уровне государства, а также аналитического инструмента Crysal Blockchain. Связан с несколькими стартапами. Являюсь автором более 70 научных публикаций по блокчейну, из которых 16 в 2023 году, включая топовые журналы и конференции. Готов поделиться своими идеями, открыт для ваших. Умею проводить исследования высокого уровня и доводить их до публикации.*

Примеры крупных направлений, над которым сейчас работаю и зову присоединяться:

1. Одной из ключевых проблем в системах блокчейн является вопрос анонимности, особенно в сделках с Bitcoin. В то время как исследователи продвинулись в решении проблемы группировки адресов пользователей и классификации пользователей, эта заявка направлена на расширение этих усилий путем введения распутывания миксеров и статистики повторного использования приватных ключей. Кроме того, мы планируем провести классификацию пользователей с использованием бустинга, нейронных сетей (графовых сетей и вложений word2vec) для выявления мошенников и незаконных действий на основе прецедентов. Улучшая процесс деанонимизации в Bitcoin, мы можем повысить прозрачность и ответственность в системе. (Хор)
2. Децентрализованные биржи стовятся все более популярными в сфере блокчейна. Однако на этих платформах часто отсутствуют системы предупреждения о мошенничестве, подобные антивирусному программному обеспечению. Это приводит к тому, что пользователи становятся жертвами мошеннических схем, таких как "rug pulls". Чтобы решить эту проблему, мы предлагаем разработку моделей машинного обучения, которые могут предоставлять предупреждения о мошенничестве в реальном времени на основе временных рядов. Начиная с "rug pulls", мы стремимся расширить область покрытия и охватить другие виды мошеннической деятельности на децентрализованных биржах. Предоставляя пользователям своевременные предупреждения о мошенничестве, мы можем повысить безопасность и надежность децентрализованных бирж.
3. Невзаимозаменимые токены (NFT) приобрели огромную популярность, и люди ценят редкость в этих цифровых коллекциях. Ранее исследователи разработали индикаторы редкости для ранжирования стоимости NFT в коллекции. Кроме того, люди часто искусственно завышают цены на NFT, чтобы получить прибыль от их продажи. Наше исследование направлено на разработку передовых индикаторов редкости, которые превосходят существующие методы и могут использоваться в качестве альтернативного подхода для обнаружения накачки цены. Точно оценивая редкость NFT и обнаруживая манипуляции ценами, мы можем способствовать прозрачности и справедливости на рынке NFT.
4. Механизмы консенсуса играют ключевую роль в системах блокчейн, обеспечивая согласие между несколькими сторонами по одному значению данных в условиях неисправных процессов. Достижение согласия при соблюдении определенных требований к производительности является фундаментальной проблемой в распределенных вычислениях. Это предложение основано на предыдущих исследованиях, которые показали применимость методов машинного обучения для оптимизации параметров блокчейна в блокчейне Solana. Мы планируем расширить этот подход на два самых популярных публичных и приватных блокчейна, Ethereum и HyperLedger Fabric. Разрабатывая испытательные стенды и применяя методы машинного обучения, мы стремимся улучшить производительность блокчейнов.

До 3-х студентов на научное руководство.

Возможно участие в грантах.

**Сергей Олегович Прилуцкий, Mixbytes (**[**https://mixbytes.io/**](https://mixbytes.io/)**)**

Направления исследований и научного руководства:

1. Темы, касающиеся zero-knowledge криптографии, zkSNARKs, а также анализаторы кода (статический, динамический анализ, фаззинг, формальная верификация)
2. Имплементации ключевых для blockchain алгоритмов: Verkle commitments, различные вариации Merkle trees, анонимизированные голосования. Анализ различных ZK-proof систем для решения типовых задач. Разработка onchain/offchain анализаторов кода, формальная верификация существующих алгоритмов

До 2-х студентов на научное руководство.

**Владимир Вячеславович Горгадзе (и коллеги из Atomyze.ru), заведующий кафедрой Блокчейн МФТИ**

Направления исследований и научного руководства на базе задач ОИС Atomyze.ru

1. В настоящее время на платформах по выпуску ЦФА не предоставляются удобные кошельки для розничных пользователей (да и сами платформы, как правило, не работают с розничными клиентами). Все операции необходимо делать через личный кабинет в web-версии, либо через мобильное приложении платформы (которое также есть не у все). Криптосообщество же уже привыкло к удобным кошелькам (отдельно стоящим, либо встроенным в браузеры.

В качестве актуальной задачи предлагается проделать интеграцию крипто-кошельков Kraken, Metamask для использования в платформе Атомайз на основе HLF (через замену ACL канала).

2. HLF является основой многих платформ, на которых требуется гибкая настройка масштабируемости для различного рода задач. Используется несколько методов для оптимизации работы HLF.

В качестве задач для НИР предлагается оптимизировать протокол исполнения кода в смарт-контрактах Hyperledger Fabric путем батчинга запросов.

3. Консенсус – наиважнейшая составляющая протокола любого публичного или полу-публичного блокчейна. Одним из наиболее устойчивых консенсусов являются консенсусы семейства BFT для асинхронных систем. Зачастую алгоритмы консенсусов разрабатываются дополнительно (как, например, SmartBFT, разработанный IBM совместно с АНО Идея) и нужнаются в тщательном тестировании.

В качестве НИР предлагается профилировка алгоритма BFT с целью выявления узких мест.

4. Кроме обеспечения устойчивой работы, алгоритм консенсуса призван поддерживать высокую произвбодительность распределенного реестра.

Предлагается исследовать возможности оптимизации алгоритма консенсуса – путем перехода на обмен хешей сообщений для согласования вместо непосредственно самих сообщений и/или путем поиска наиболее оптимальных параметров настроек (например, методами ML).

Направления исследований и научного руководства на базе задач Сбера:

1. Разработать методы сбора датасетов для ML задач в блокчейне и подготовка открытых бенчмарков
2. Анализ транзакций для поиска связанных транзакций в бриджах
3. Классификация пользователей DeFi по поведению (AML)
4. Прогнозирование цен криптоактивов с учетом состава держателей и их поведения
5. Анализ риска займа (риск, прибыль, лонг/шорт)
6. Анализ возможности применения кредитных протоколов для лонг и шорт стратегий
7. Связь динамических кластеров, поведения пользователей и качества прогноза цен

До 4-х студентов на научное руководство.

Успешным кандидатам могут быть предложены стажировки или трудоустройство.

**Максим Александрович Рябов, технический директор токенизационной платформы ATME (**[**https://www.atme.com/**](https://www.atme.com/)**)**

1. Исследование динамики поведения клиентов в разных блокчейнах. Как эволюционирует поведение среднего пользователя, количество транзакций,количество контрагентов, количество сервисов, площадок, бирж которыми пользуется средний пользователь.

Создать инструмент анализа изменения характера поведения пользователей одного из топ-20 блокчейнов с течением времени. Определить принципы кластеризации, время жизни кластеров, распределение кошельков по типам схожего поведения и их количественный рост/спад во времени, выделение платежных операций. Визуализация графов всех транзакций, по кошелькам отвечающим критериям активности. Анализ с помощью графов: определение кошельков бирж, платформ.

1. Анализ количества транзакции в количестве и объеме операций и поиск зависимостей от значимых событий в экономике, политике, в разрезе по типам крипто активов (стейблкоины, гранды (BTC, ETH), криптомелочь). Разработка подхода к кластеризации кошельков по географическому признаку. Увеличение точности подхода на основе балансов локальных токенов (которые популярны в конкретной стране, регионе) и связанности локально определяемых кошельков с окружением до +2, +3 ребер графа.
2. Анализ существующих подходов к оценке количества кошельков открытых в каждой отдельной стране. Оценка количества пользователей на основе кол-ва кошельков. Оценка пользователей по сумме криптоактивов. Динамика количества разовых кошельков. Всплески регистрации разовых кошельков в моменты - начало военных действий, неожиданное повышение ставки ЦБ, банкротство крупного банка, политических кризис в стране, военный мятеж.
3. Создать метод расчета количества потерянных кошельков в публичных чейнах, анализ кол-ва заблокированных активов на таких кошельках. Сделать выводы как могут повлиять неожиданно найденный доступ к потерянным кошелькам активам на рыночные цены этих активов. Определить порог потерянных активов к непотерянным в рамках одного конкретного актива, превышение которого несет риски обнуления стоимости актива. Эксперимент: смоделировать цену на BTC, если большой молчащий крипто кошелек эпохи Сатоши решит продать все активы.
4. Абстракция кошельков пользователей (работа без подписи, регулярные выплаты)
5. DEFI - описать концепт создания DEFI площадки с приватным допуском, после регистрации и KYC. Анализ подобных решений. Плюсы, минусы.
6. Успешные концепции ютилити токенов. Создать классификатор видов юнит экономики для платформенных, сервисных токенов. Разработать подход к оценке количества успешных токенов в рамках каждого класса.
7. Облачная демократия и блокчейн. Большая тема, много тем, вопросов. Явный конфликт прогресса здесь с органами централизованной власти. Можно развить в несколько больших работ если есть интерес магистрантов и МФТИ не против брать риск

До 3-х студентов на научное руководство.

Успешным кандидатам могут быть предложены стажировки или трудоустройство.

**Александр Александрович Николаев, Symbiosis.Finance (**[**https://symbiosis.finance/**](https://symbiosis.finance/)**)**

Профессиональные и научные интересы лежат вокруг публичных блокчейн сетей, и вопросах связанных с улучшением пользовательского опыта, и продвинутых инженерных задачах на стыке криптографии и смарт контрактов.

Направления исследований и научного руководства:

1. AA abstraction кошельки и модули для них, большой тренд о том как сделать пользовательский опыт более человечным без необходимости помнить сид фразы, приватные ключи
   * Альтернативный мемпул
   * Модули безопасности таких кошельков
2. Кроссчейн взаимодействия, упрощение кроссчейн транзакций и взаимодействии приложений на разных чейнах.

До 2-х студентов на научное руководство.

Успешным кандидатам могут быть предложены стажировки или трудоустройство.

**Павел Шувалов, CTO и основатель нескольких стартапов, сооснователь проекта re:doubt (**[**https://github.com/shuva10v**](https://github.com/shuva10v)**)**

Направления исследований и научного руководства:

1. Анализ данных блокчейна
2. Исследовательские и прикладные задачи по развитию платформы TON

Одного студента на научное руководство.

**Алексей Вячеславович Курочкин, Ринат Фаритович Шакиров, Код Безопасности (**[**https://www.securitycode.ru/**](https://www.securitycode.ru/)**)**

В сфере цифровой экономики (в частности, и в блокчейн сфере) всё чаще возникают задачи, решение которых зачастую невозможно с применением классических криптографических механизмов. Для решения некоторых задач используются пороговые механизмы (частным случаем которых являются пороговые подписи), доказательства нулевого знания слепые подписи и протоколы конфиденциальных вычислений. Вышеуказанные механизмы применяются для решения задач обеспечения криптографической безопасности, например: дистанционного голосования, смарт-контрактов, электронных аукционов, запросов к базам данных, банковских взаимодействий.

В связи с этим предлагаются следующие направления исследований:

* исследование возможности безопасного применения слепой подписи в блокчейн сфере;
* создание эффективной масштабируемой пороговой подписи;
* схемы выработки общего секрета с аутентификацией и защитой от атак вид «чтение вперёд» и «чтение назад»;
* исследование возможности безопасного эффективного применения протоколов конфиденциального вычисления в блокчейн сфере;
* применимость атаки на изогении в схеме «Форзиция» (протокол выработки общего ключа на основе аппарата изогений суперсингулярных эллиптических кривых).

До 2-х студентов на научное руководство.