# Формальная верификация в блокчейн-системах

Рогозин Даня
МГУ им. Ломоносова
Serokell OU

# Что такое блокчейн?

- Блокчейн - это структура данных, представляющая собой последовательность элементов, каждый из хранит хэш предыдущего элемента. Произвольный элемент данной последовательности называется блоком.
- Под хэшем мы подразумеваем элемент области значений криптографической хэш-функции (алгоритма, преобразующего те или иные данные в байтовую строку фиксированной длины)
- Блокчейн-система - это децентрализованная база данных, в которой транзакции в рамках этой базы хранятся в блоках. А уже данные блоки образуют блокчейн.
- Алгоритм консенсуса - это способ консолидации между участниками сети. Кого и как консолидировать, это зависит от предметной области. Независимо от предметной области все участники сети должны на одинаковых правах видеть историю транзакций.

# Пример, что у всех на слуху. Bitcoin (да-да, он самый).

- Bitcoin - это одна из самых первых и самых известных криптовалют;
- Использует алгоритм консенсуса доказательства работы (proof of work), то есть добыча каждого блока (он же майнинг) должна сопровождаться свидетельством того, что данный участник сети сгенерировал данный блок, используя свои большие вычислительные мощности;
- Каждый блок состоит из заголовка (включающего хэш предыдущего блока), списка транзакций и собственно доказательства работы.

# Недостатки в системе Bitcoin

- Есть два основных недостатка, которые можно рассматривать в целом как недостаток proof of work консенсуса;
- Недостатки: блок в системе Bitcoin создается каждые 10 минут, а расходы электроэнергии примерно равны недельным расходам на инфраструктуру жилого дома. Отсюда мы имеем дело с далеко идущими энергетическими и экологическими последствиями.
- Нарушение принципа децентрализации: чем больше твои мощности, тем больше шансов получить блок. На практике, чем мощнее майнинговые фермы, то больше возможностей у фермера получить блок и доход от него, который формируется в результате комиссий на транзакции. Иными словами, данную децентрализованную сеть сравнительно легко со временем централизовать.

# Криптовалюта Cardano

- Наша компания долго работала над Cardano, пока не перестала работать.
- Используется Proof of stake консенсус, иными словами метод доказательства доли владения. Право на генерацию блока определяется не мощностью железа, а финансовой долей, если угодно, пакетом акций.
- В общем случае это не решает проблему монополизации. В результате был разработан собственный безопасный PoS алгоритм консенсуса Ouroboros.

# Выбор счастливчика на пальцах.

- Мы делим кусок временной шкалы (эпоху) на слоты. Без ограничения общности, положим один слот равным одной минуте.
- Берем список кандидатов, который извлекается из родового блока. Кандидату в эпохе соответствует свой слот с некоторым сгенерированным блоком, иными словами, определяются лидеры слотов.
- При смене эпохи меняется начальный блок со списком новых кандидатов.
- Кандидаты одной эпохи специальным образом разыгрывают лотерею, чтобы определить кандидатов на будущую эпоху, используя специальные алгоритмы с рандомайзерами (смотрите подробнее алгоритм под названием Follow The Satoshi).

# Другие примеры использования блокчейн-технологий.

- Земельные реестры;
- Контроль прав сотрудников;
- Отслеживание за академической успеваемостью;
- DevOps процессы (для IT команд);
- Страховки;
- Аукционы;
- Et cetera.

# Обобщенная модель блокчейн-системы

- Что значит предъявить обобщенную модель блокчейн-системы?
- Это означает обобщение базовых определений, лежащих в основе блокчейн системы, то есть абстрагирование их основных свойств от конкретных реализаций. То есть надо понять, что такое блок, что такое транзакция, что такое валидация транзакции (и т.д.) в общем случае, независимо от того, какие именно мы действия совершаем в наших транзакциях и что именно мы храним в блоках.
- Ясно, что при таком подходе повышается степень абстракции и требования к строгости формулировок.

# Snowdrop

- Фреймворк, предназначенный для проектирования блокчейн-систем;
- В основе лежит обобщенная модель функционала блокчейн-системы;
- Реализован на Haskell. Система типов Haskell достаточно сильна, чтобы писать и поддерживать код, обладающий достаточно высокой степенью абстракции и общности.
- Функционал разбит на независимые друг от друга части. В частности, обобщенная обработка блоков и валидация транзакции почти никак не пересекаются.
- Интеграция с проектом Disciplina от компании Teach Me Please.

# Применение методов формальной верификации.

- Верификация необходимых нам свойств производится на языке программирования Agda.
- Система типов языка Agda системы типов Haskell (в основе вариант теории типов Мартин-Лёфа), что позволяет:
- Во-первых, задавать алгебраические аксиомы и свойства базовых вычислений.
- Аналогичным образом задавать алгебраические законы для вычислений, которые имеют read-only доступ к текущему состоянию системы.
- Предъявить аксиомы для read-only доступа к состоянию системы, для тех ситуаций, когда явно переданы текущие изменения системы.
- Задавать обобщенные свойства гетерогенных хранилищ.
- Доказывать оценки на глубину валидации транзакций.

# Дальнейшие планы

- Релиз запланирован на конец 2018 года. Ориентировочно, ноябрь.
- Релиз будет сопровождаться документацией и подробной статьей, где будет изложена верификация базовых свойств обобщенной блокчейн-системы, реализованной в Snowdrop.
- В планах создание альтернативного клиента для Cardano, ориентировочно, начало 2019 года.
- Более того, есть масса открытых на данный момент вопросов по верификации основных свойств предложенной системы. Например, (желательно, корректная) денотационная семантика остается на данный момент неформализованной.

# Концептуальные соображения

- Ранее модели и спецификации блокчейн-систем не предлагались в обобщенном виде. Как правило разработчики и исследователи в данных областях решают более узкие задачи, продиктованные настоящим моментом.
- Обобщающий подход может давать более долгосрочные и универсальные решения, и во многом универсальность и долгосрочность этих решений будет напрямую зависеть от того, какая за данным подходом стоит теория, а вопросы теории как раз и решаются в данной работе (теория базового вычисления, вычисление с read-only доступом к состоянию системы и так далее).

# Концептуальные соображения

- Основная методология - это формализованная математическая формализация основных компонент системы с доказуемо верифицированным свойствами. При этом желательно, чтобы предложенная формализация функционала мало отличалась от реализации того, что есть на продакшене.
- С инженерной точки зрения, связка Agda-Haskell выглядит вполне оправданной
- С теоретической точки зрения, мы стоим на плечах гигантов, используя достижения конструктивной математической логики (конструктивной теории доказательств, в частности).

# Концептуальные моменты и итоги.

- А само обобщение свойств и операций в блокчейн системе предполагает формулировку достаточно оригинально устроенных алгебраических теорий, для которых вопросы теоретико-модельного характера также открыты.
- Если указанные выше вопросы мы сможем решить, то это будет существенный шаг вперед в построении формально обобщенной теории блокчейн-систем.
- Для этого нужна завершенная теория, над завершением которой мы сейчас и работаем.

# Спасибо за внимание!